



DEPARTMENT OF THE NAVY
BUREAU OF NAVAL PERSONNEL
5720 INTEGRITY DRIVE
MILLINGTON, TN 38055-0000

BUPERSINST 5230.8

BUPERS-07

29 SEP 2011

BUPERS INSTRUCTION 5230.8

From: Chief of Naval Personnel

Subj: BUREAU OF NAVAL PERSONNEL CONTINUITY AND CONTINGENCY
PLANNING AND SUSTAINMENT PROGRAM

Ref: (a) OMB Circular A130, Revised
(b) OPNAVINST 3030.5B
(c) SECNAVINST 3030.4C
(d) Federal Continuity Directive 1 of Feb 2008
(e) NIST Special Publication 800-34, Rev 1 of May 2010

Encl: (1) Definitions
(2) National and DON Essential Functions
(3) Differences in Plans
(4) Types of Plans
(5) Relationships between Plans

1. Purpose. To establish an overarching Bureau of Naval Personnel (BUPERS) continuity and contingency planning and sustainment program to ensure BUPERS codes and subordinate activities develop and maintain a continuity of operations (COOP) plan, business continuity plans (BCPs), a disaster recovery plan (DRP), and information system contingency plans (ISCPs). The development of these plans is necessary to ensure BUPERS and its subordinate commands are prepared to support and or perform Department of Navy (DON) mission essential functions (MEFs) and to facilitate business continuity during recovery from a disruptive event, up to the time when the organization returns to normal operations. It is important to note that there are numerous types of plans associated with supporting the recovery from a disruptive event; this instruction is focused on the plans that address the ability to support MEFs (the COOP plan), to perform other important, but less critical business processes (a BCP), to reconstitute information systems (IS) at an alternate location (the DRP), and the requirements and procedures to recover a single information system (an ISCP).

2. Background. Per references (a), (b), and (c), continuity planning is a critical component of readiness. Navy commands must not only be prepared to support and execute DON MEFs, but

also have a plan to continue other important business functions while operating in a degraded state. Enclosures (1) through (5) are provided to minimize confusion regarding the differences between COOP plan, BCP, DRP, ISCP and other emergency-related plans, since the term "COOP Plan" is often incorrectly used to describe an all-encompassing disaster recovery plan. The primary characteristic of a COOP plan is the support and or execution of carefully identified and vetted MEFs. MEFs are typically agency-level government functions that are mandated by law, presidential directive, or executive order that support national essential functions (NEFs). MEFs can be properly identified by using the guidance provided in reference (d).

3. Applicability. Continuity and contingency planning is applicable to all BUPERS codes and subordinate activities.

4. Action

a. All BUPERS codes and subordinate activities shall:

(1) Be ultimately accountable for the development, maintenance, and effectiveness of the continuity and contingency plans;

(2) Designate a continuity coordinator that will be responsible for coordinating the development and maintenance of the continuity and contingency plans;

(3) Submit approved continuity and contingency plans to the BUPERS Command Information Officer (BUPERS-07) not less than annually; and

(4) Ensure subordinate commands and activities take the appropriate steps to plan and prepare for disruptive events.

b. Designated Continuity Coordinators shall:

(1) Coordinate the development and maintenance of their command's/code's continuity and contingency plans per the guidance provided by the BUPERS Continuity Coordinator (BUPERS-07);

(2) Participate in BUPERS continuity and contingency plan coordination efforts led by the BUPERS Continuity Coordinator (BUPERS-07);

(3) Provide continuity and contingency plans to the BUPERS Continuity Coordinator (BUPERS-07) for review and endorsement prior to approval; and

(4) Convene coordination efforts to oversee the development of continuity and contingency plans of subordinate commands and activities.

c. BUPERS Continuity Coordinator (BUPERS-07) shall:

(1) Coordinate the development and maintenance of BUPERS continuity and contingency plans per the guidance set forth in reference (b); using references (c), (d), and (e) for amplifying guidance;

(2) Convene continuity and contingency plan development coordination efforts to include the continuity coordinators from individual BUPERS codes and subordinate activities;

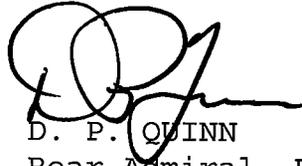
(3) Provide specific guidance on the required content and format of continuity and contingency plans; and

(4) Review and endorse individual BUPERS codes and subordinate activities continuity and contingency plans.

5. Point of Contact. BUPERS Continuity Coordinator (BUPERS-07); all correspondence routed to e-mail address BUPERS_COOP@navy.mil.

6. Records Management. Records created as a result of this instruction, regardless of media and format, shall be managed per Secretary of the Navy Manual M-5210.1 of November 2007.

7. Reports. Reporting requirements contained in this instruction are exempt from reports control per SECNAVINST M-5214.1 of December 2005.



D. P. QUINN
Rear Admiral, U.S. Navy
Deputy Chief of Naval Personnel

Distribution:
Electronic only, via BUPERS Web site
<http://www.npc.navy.mil>

DEFINITIONS

Business Continuity Plan (BCP) - The documentation of a predetermined set of instructions or procedures that describe how an organization's mission and business processes will be sustained during and after a significant disruption. (Reference (e))

Catastrophic Emergency - Any incident, regardless of location, that results in extraordinary levels of mass casualties, damage, or disruption severely affecting the U.S. population, infrastructure, environment, economy, or government functions. (Reference (d))

Continuity - An uninterrupted ability to provide services and support, while maintaining organizational viability, before, during, and after an event. (Reference (d))

Continuity of Government (COG) - A coordinated effort within each branch of government (e.g., the Federal Government's executive branch) to ensure that NEFs continue to be performed during a catastrophic emergency. Note: this term may also be applied to non-Federal governments. (Reference (d))

Continuity of Operations (COOP) - An effort within individual agencies to ensure they can continue to perform their MEFs and Primary MEFs (PMEFs) during a wide range of emergencies, including localized acts of nature, accidents, and technological or attack-related emergencies. (Reference (d))

Continuity of Operations (COOP) Plan - A predetermined set of instructions or procedures that describe how an organization's MEFs will be sustained within 12 hours and for up to 30 days as a result of a disaster event before returning to normal operations. (Reference (e))

Essential Functions - The critical activities performed by organizations, especially after a disruption of normal activities. There are three categories of essential functions: NEFs, PMEfs, and MEFs. (Reference (d))

29 SEP 2011

Mission Essential Functions (MEFs) - The limited set of agency-level Government functions that must be continued throughout, or resumed rapidly after, a disruption of normal activities. (Reference (d))

National Essential Functions (NEFs) - The eight functions the President and the Nation's leadership will focus on to lead and sustain the Nation during a catastrophic emergency; NEFs, therefore, must be supported by COOP and continuity of government capabilities. (Reference (d))

Primary Mission Essential Functions (PMEFs) - Those department and agency MEFs, validated by the National Continuity Coordinator, which must be performed in order to support the performance of NEFs before, during, and in the aftermath of an emergency. PMEFs need to be continuous or resumed within 12 hours after an event and maintained for up to 30 days or until normal operations can be resumed. (Reference (d))

29 SEP 2011

NATIONAL AND DON ESSENTIAL FUNCTIONS

National Essential Functions (NEFs)

1. Ensuring the continued functioning of our form of Government under the Constitution, including the functioning of the three separate branches of government.
2. Providing leadership visible to the Nation and the world, and maintaining the trust and confidence of the American people.
3. Defending the Constitution of the United States against all enemies, foreign and domestic, and preventing or interdicting attacks against the United States or its people, property, or interests.
4. Maintaining and fostering effective relationships with foreign nations.
5. Protecting against threats to the homeland and bringing to justice perpetrators of crimes or attacks against the United States or its people, property or interests.
6. Providing rapid and effective responses to and recovery from the domestic consequences of an attack or other incident.
7. Protecting and stabilizing the Nation's economy and ensuring public confidence in its financial systems.
8. Providing for critical Federal Government services that address the national health, safety, and welfare needs of the United States.

DON Mission Essential Functions (MEFs)

1. Support the Secretary of the Navy (SECNAV).
2. Support the Chief of Naval Operations (CNO) and Commandant of the Marine Corps (CMC).
3. Respond to tasking and provide information necessary to facilitate Navy operations worldwide.

4. Support requirements established in the Office of the Secretary of Defense and Chairman Joint Chiefs of Staff continuity directives and plans.
5. Execute Department of the Navy's (DON'S) responsibilities under Title 10, United States Code.
6. Provide command and control from all units to the SECNAV, CNO, and CMC, and back.

Per references (b) and (c), "DON MEFs also support NEFs and primary MEFs as delineated in National Security Presidential Directive 51 and Homeland Security Presidential Directive 20 and Department of Defense directives."

29 SEP 2011

DIFFERENCES IN PLANS

(APPENDIX C FROM REFERENCE (E))

What are the differences among a continuity of operations plan (COOP), a business continuity plan (BCP), a critical infrastructure protection (CIP) plan, a disaster recovery plan (DRP), an information system contingency plan (ISCP), a cyber incident response plan, and an occupant emergency plan (OEP)?

Organizations require a suite of plans to prepare themselves for response, continuity, recovery, and resumption of mission and business processes and information systems in the event of a disruption. Each plan has a specific purpose and scope; however, because of the lack of standard definitions for these types of plans, in some cases, the scope of actual plans developed by organizations may vary from the following basic descriptions.

A COOP is required by Homeland Security Presidential Directive (HSPD) - 20, National Security Presidential Directive (NSPD) - 51, National Continuity Policy and Federal Continuity Directive (FCD) - 1, Federal Executive Branch National Continuity Program and Requirements for sustaining an organization's (usually a headquarters element) mission essential functions (MEF) at an alternate site and performing those functions for up to 30 days before returning to normal operations.

A BCP addresses sustaining mission and business processes and the information systems that support those mission and business processes during and after a significant disruption. BCPs are often developed at the organization's field level or for mission and business processes that are not prioritized as mission essential.

A CIP plan is a set of policies and procedures that serve to protect and recover those components of the national infrastructure that are deemed so vital that their loss would have a debilitating effect of the safety, security, economy, and or health of the United States.

29 SEP 2011

DIFFERENCES IN PLANS

(APPENDIX C FROM REFERENCE (E))

A DRP refers to an information system-focused plan designed to restore operability of one or more information systems at an alternate site after a major disruption usually causing physical damage to the original data center.

An ISCP provides recovery and resumption procedures for a single information system resulting from disruptions that do not necessarily require relocation to an alternate site.

A Cyber Incident Response Plan establishes procedures to enable security personnel to identify, mitigate, and recover from cyber attacks against an organization's information system(s).

An OEP provides directions for facility occupants to follow in the event of an emergency situation that threatens the health and safety of personnel, the environment, or property.

29 SEP 2011

TYPES OF PLANS

(TABLE 2-2 FROM REFERENCE (E))

Plan	Purpose	Scope	Plan Relationship
Business Continuity Plan (BCP)	Provides procedures for sustaining mission/business operations while recovering from a significant disruption.	Addresses mission/business processes at a lower or expanded level from COOP MEFs.	Mission/business process focused plan that may be activated in coordination with a COOP plan to sustain non-MEFs.
Continuity of Operations (COOP) Plan	Provides procedures and guidance to sustain an organization's MEFs at an alternate site for up to 30 days; mandated by federal directives.	Addresses MEFs at a facility; information systems are addressed based only on their support of the mission essential functions.	MEF focused plan that may also activate several business unit-level BCPs, ISCPs, or DRPs, as appropriate.
Crisis Communications Plan	Provides procedures for disseminating internal and external communications; means to provide critical status information and control rumors.	Addresses communications with personnel and the public; not information system-focused.	Incident-based plan often activated with a COOP or BCP, but may be used alone during a public exposure event.
Critical Infrastructure Protection (CIP) Plan	Provides policies and procedures for protection of national critical infrastructure components, as defined in the National Infrastructure Protection Plan.	Addresses critical infrastructure components that are supported or operated by an agency or organization.	Risk management plan that supports COOP plans for organizations with critical infrastructure and key resource assets.
Cyber Incident Response Plan	Provides procedures for mitigating and correcting a cyber attack, such as a virus, worm, or Trojan horse.	Addresses mitigation and isolation of affected systems, cleanup, and minimizing loss of information.	Information system-focused plan that may activate an ISCP or DRP, depending on the extent of the attack.
Disaster Recovery Plan (DRP)	Provides procedures for relocating information systems operations to an alternate location.	Activated after major system disruptions with long-term effects.	Information system-focused plan that activates one or more ISCPs for recovery of individual systems.
Information System Contingency Plan (ISCP)	Provides procedures and capabilities for recovering an information system.	Addresses single information system recovery at the current or, if appropriate alternate location.	Information system-focused plan that may be activated independent from other plans or as part of a larger recovery effort coordinated with a DRP, COOP, and/or BCP.
Occupant Emergency Plan (OEP)	Provides coordinated procedures for minimizing loss of life or injury and protecting property damage in response to a physical threat.	Focuses on personnel and property particular to the specific facility; not mission/business process or information system-based.	Incident-based plan that is initiated immediately after an event, preceding a COOP or DRP activation.

29 SEP 2011

RELATIONSHIPS BETWEEN PLANS

