



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

BUPERSINST 5230.8A
BUPERS-07

07 JUN 2013

BUPERS INSTRUCTION 5230.8A

From: Chief of Naval Personnel

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

Ref: (a) OPNAVINST 3030.5B
(b) Federal Continuity Directive 1 of Feb 2008
(c) Federal Continuity Directive 2 of Feb 2008
(d) NIST Special Publication 800-34, Rev 1 of May 2010
(e) U.S. Navy Regulations 1990, as amended

Encl: (1) Annex Map
(2) Definitions
(3) National, DoD, and DON Essential Functions
(4) Differences in Plans
(5) Types of Plans

1. Purpose. To expand the Bureau of Naval Personnel (BUPERS) continuity and contingency program by refining roles and responsibilities, outlining the policy governing annual testing and formal plan reviews, and establishing a mechanism to support the timely development, approval, and maintenance of continuity and contingency planning documents.

2. Cancellation. BUPERSINST 5230.8.

3. Background. This instruction serves as the first revision to BUPERS continuity and contingency planning and sustainment program. The primary focus of the original instruction led to the initial development of an overarching BUPERS continuity of operations (COOP) plan, individual code/command business continuity plans (BCPs), and various information system contingency plans (ISCPs). The development and periodic review of these plans are necessary to ensure BUPERS and its subordinate commands are prepared to support and or perform Department of Navy (DON) mission essential functions (MEFs) (which are mapped to the Department of Defense (DoD) MEFs) and locally identified business essential functions (BEFs) to facilitate mission/business continuity during recovery from a

07 JUN 2013

disruptive event, up to the time when the organization returns to normal operations.

4. Discussion

a. Reference (a) requires all Navy echelon 2 commands to develop a COOP plan. Per reference (b), a COOP plan is developed to ensure the organization is prepared to perform identified MEFs, which are defined as "the limited set of agency-level Government functions that must be continued throughout, or resumed rapidly after, a disruption of normal activities." Reference (c) further defines MEFs as "those functions that enable an organization to provide vital services, exercise civil authority, maintain the safety of the public, and sustain the industrial and economic base, during the disruption of normal operations." MEFs are typically agency-level Government functions mandated by law, presidential directive, or executive order that support national essential functions (NEFs).

b. Due to the desire to also perform less critical but important business functions in a post-disaster or disruptive environment, BUPERS has elected to incorporate the development of business continuity plans (BCPs) in parallel with the COOP planning effort. While the COOP plan addresses the performance of MEFs, BCPs address the performance of BEFs, which reference (d) broadly defines as "procedures for sustaining mission/business operations while recovering from a significant disruption." The BUPERS-specific definition of a BEF is as follows: BEFs are those carefully selected organizational functions that are desired to be performed continuously or resumed rapidly (within 2 weeks) after a disruptive event to support the mission, to avoid significant negative impact, or to facilitate recovery operations. BEFs do not meet the requirements to become a MEF, but they are identified as important enough to the business that the organization's leadership is willing to allocate resources to plan for, execute, and sustain them to ensure business continuity during and or following a disruptive event.

c. The organization's continuity and contingency planning effort should include not only a COOP plan and BCPs, but also the development of other plans that serve to support the performance of essential functions as well as those that focus

07 JUN 2013

on emergency and recovery operations. For example, according to reference (d), a typical continuity and contingency planning suite also includes a crisis communications plan, an occupant emergency plan (OEP), and disaster recovery plan (DRP).

5. Policy

a. The documents that comprise the BUPERS continuity and contingency planning suite shall be developed, approved, and maintained individually in accordance with the modular approach depicted in enclosure (1).

b. Continuity and contingency planning documentation shall be centrally stored and managed in the Navy's official document repository (i.e., Total Records Information Management). Hardcopies shall be stored by the continuity coordinators and by other key personnel, as necessary, to facilitate business continuity.

c. Continuity and contingency planning documentation shall be reviewed for accuracy semi-annually (once during January - February and once during July - August).

d. Continuity and contingency plans shall be tested annually. Test plans, which will include test dates and scope, shall be developed by the command continuity coordinator in close coordination with command leadership. Annual tests should increase in scope and complexity as the continuity and contingency program matures.

e. All continuity and contingency plans shall address activation criteria and activating authority.

f. The Deputy, Chief of Naval Personnel (DEP CHNAVPERS) shall be notified as soon as practicable, via the applicable chain, whenever:

(1) A continuity or contingency plan is activated;

(2) There is an inability to perform a MEF or a BEF, under normal operations or during a disruptive event.

g. The continuity and contingency planning program was primarily developed to address mission and business resiliency

07 JUN 2013

of BUPERS and its subordinate commands located on the Millington campus. Nothing in this instruction or in its supporting annexes shall conflict, interfere, supersede, or otherwise inhibit the Commanding Officer, Naval Support Activity Mid-South from performing his or her duties outlined in article 0802 of reference (e).

6. Applicability. The continuity and contingency planning and sustainment effort is applicable to all BUPERS codes and subordinate activities located on the Millington campus only. BUPERS Washington, D.C. codes will be included in the OPNAV N1 continuity of operations plan.

7. Action

a. All leaders of BUPERS codes and subordinate activities shall:

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

(2) Ensure recall rosters are kept up to date and made available only to those with a need to know;

(3) Be familiar with applicable continuity and contingency plans, to include criteria for plan activation and the MEFs and BEFs performed or supported;

(4) Designate a continuity coordinator;

(5) Ensure continuity and contingency planning efforts are timely and accurate;

(6) Ensure active participation in annual testing and the semi-annual review of continuity and contingency plans and artifacts;

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

(8) Ensure continuity and contingency activities are well communicated up and down the chain of command, prior to,

07 JUN 2013

during, and after a disruptive event, to the maximum extent practicable.

b. Designated continuity coordinators shall:

(1) Act as a liaison for their organization and coordinate the development and maintenance of their command/code continuity and contingency plans per the guidance provided by the BUPERS Continuity Coordinator;

(2) Participate in BUPERS continuity and contingency planning and testing coordination efforts led by the BUPERS Continuity Coordinator.

c. BUPERS Command Information Officer (BUPERS-07), shall:

(1) Be responsible for the overall management and health of the BUPERS Continuity and Contingency Program;

(2) Designate the BUPERS Continuity Coordinator in writing.

d. BUPERS Continuity Coordinator, Navy Personnel Command (NAVPERSCOM) Continuity Coordinator; Navy Recruiting Command (NAVCRUITCOM) Continuity Coordinator; and Navy Manpower Analysis Center (NAVMAC) Continuity Coordinator shall:

(1) Coordinate the development and maintenance of BUPERS continuity and contingency plans to include annual testing and the semi-annual review of continuity and contingency plans and artifacts;

(2) Ensure that the semi-annual review of BUPERS continuity and contingency plans and artifacts begins no earlier than 1 January and 1 July and are completed by 28 February and 31 August respectively;

(3) Plan for and coordinate annual testing events. Submit test plan to command leadership for review and approval at least 2 months prior to test start date and provide test results and lessons learned to all participants within 2 weeks of test conclusion.

07 JUN 2013

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

9. Records Management. Records created as a result of this instruction, regardless of media and format, shall be managed per Secretary of the Navy (SECNAV) Manual M-5210.1 of January 2012.

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



C. A. COVELL

Rear Admiral, U.S. Navy

Deputy Chief of Naval Personnel

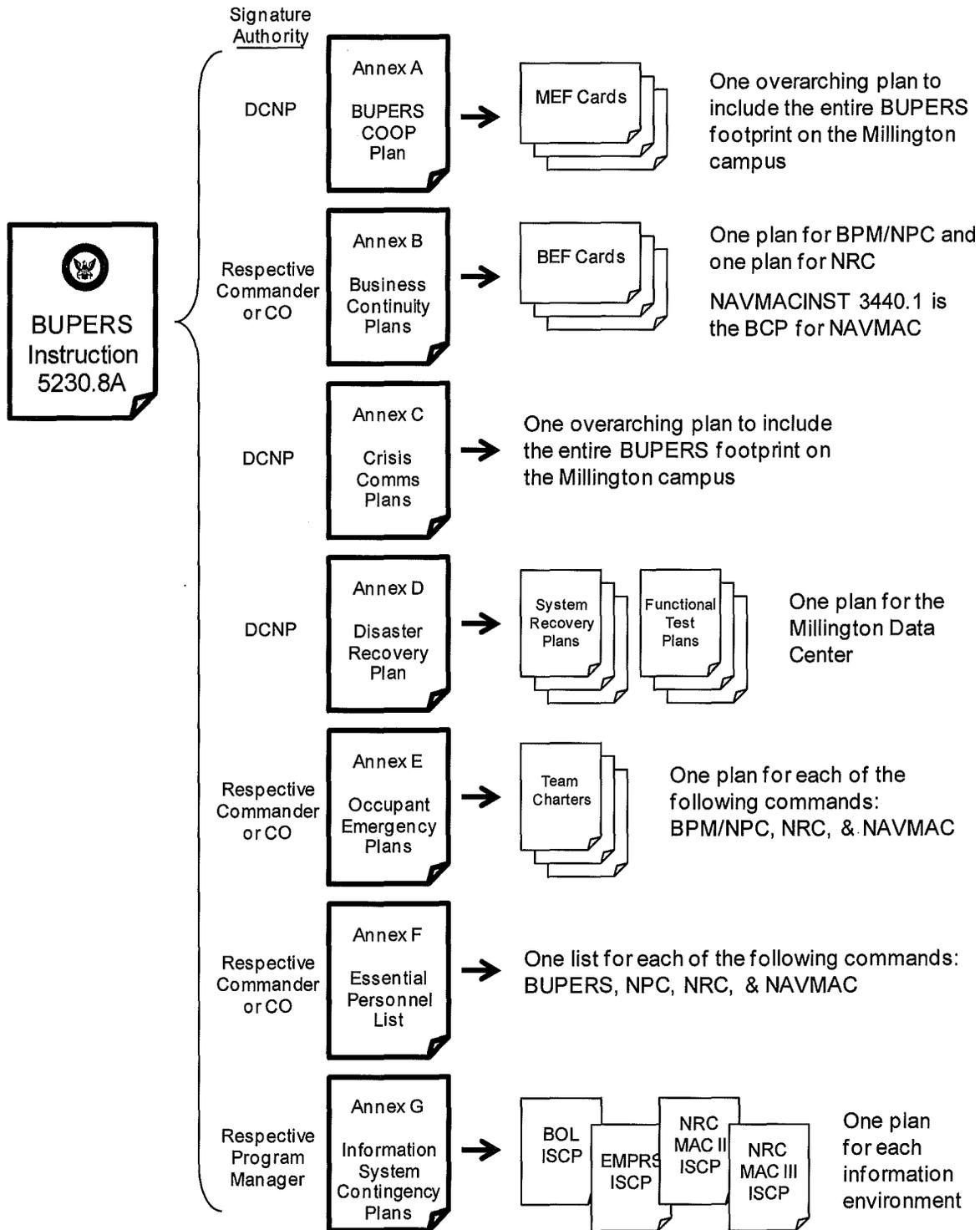
Distribution:

Electronic only, via BUPERS Web site

<http://www.npc.navy.mil>

07 JUN 2013

ANNEX MAP



07 JUN 2013

DEFINITIONS

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

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 (b))

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

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 (b))

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 (b))

Continuity of Operations (COOP) Plan - A predetermined set of instructions or procedures that describes 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 (d))

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 (b))

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 (b))

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 COG capabilities. (Reference (b))

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 (b))

07 JUN 2013

NATIONAL, DOD, 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.

DoD Primary Mission Essential Functions (PMEFs)

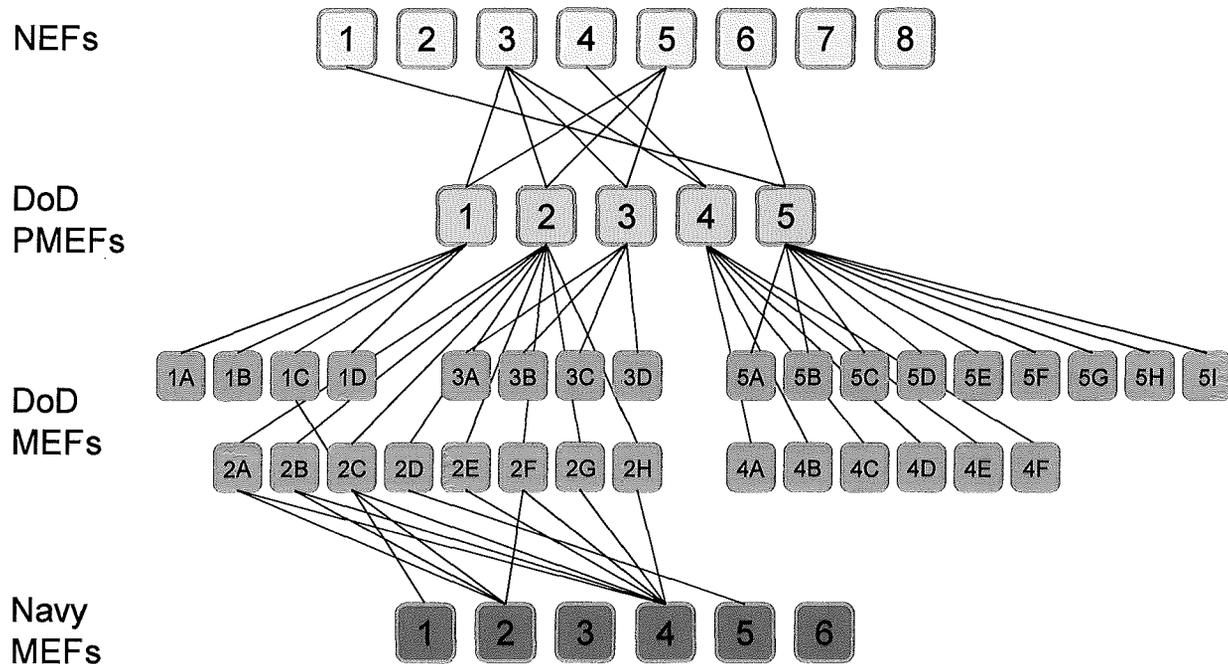
1. Formulate National Defense Policy
2. Protect and Defend the Country
3. Maintain World Wide Situational Awareness
4. Promote National Security
5. Conduct Domestic Emergency Response

07 JUN 2013

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 world wide.
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 reference (a), "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."



07 JUN 2013

DIFFERENCES IN PLANS**(APPENDIX C FROM REFERENCE (D))**

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.

07 JUN 2013

DIFFERENCES IN PLANS

(APPENDIX C FROM REFERENCE (D))

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.

TYPES OF PLANS

(TABLE 2-2 FROM REFERENCE (D))

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.