DEPARTMENT OF THE NAVY
NAVY RECRUITING DISTRICT, PORTLAND
7028 N.E. 79TH COURT
PORTLAND, OREGON 97218-2813

NAVCRUITDISTPORTLANDINST 5239.2B
SYSAD
16 Dec 13

NAVCRUITDIST PORTLAND INSTRUCTION 5239.2B

Subj: INFORMATION SYSTEMS CONTINGENCY PLAN

Ref: (a) SECNAVINST 5239.3B
(b) OPNAVINST 5239.1C
(c) COMNAVCRUITCOMINST 5239.1A

Encl: (1) Navy Recruiting District Portland information systems contingency plan
(2) Memorandum of Understanding

1. Purpose. This contingency plan details operational requirements for specific information systems (IS), telecommunications equipment, and hardware and software. It includes a relocation Memorandum of Understanding (MOU) between Navy Recruiting District (NRD) Portland and Navy Operational Support Center (NOSC) Portland, in order to ensure NRD Portland can continue its mission with minimal impact in a disrupted operating environment.

2. Scope. This contingency plan establishes procedures and outlines responsibilities to accomplish limited mission functions in the event of an unexpected service interruption that degrades NRD Portland local area network (LAN) operations and/or availability. A backup procedure for software assets and limited duplication of hardware resources is the single most important element in establishing an effective loss-control program. Through effective restoration planning and well-defined contingency actions, continued IS mission critical operations are possible with only limited systems degradation. System restoration actions may take place on-site or may require relocation to an alternate site. This decision is based on resource availability, the scope of the contingency and operational need to preserve data confidentiality, software support integrity, and service availability. The Designated Approving Authority (DAA), with advice from the NRD Portland Information Assurance Officer (IAO), will direct all NRD Portland LAN contingency relocation or restoration efforts.

3. Applicability. References (a) through (c) require each Department of Navy (DON) activity dependent upon IS operations to develop a contingency plan for recovery of IS for which an unplanned disruption of service would critically impact mission accomplishment.

4. Policy

a. The establishment of an effective, well defined IS contingency plan is an integral part of the command's overall IS security posture. Special emphasis will be placed on personnel actions and hardware/software resources necessary to facilitate mission accomplishment in the event of an unplanned IS service interruption. Specific IS contingency measures will address:

(1) Limited loss of IS capability. This is loss of IS capabilities for only a limited period of time, with little or no operational impact. Risks include:

(a) Failure of peripheral hardware
(b) Temporary power interruptions
(c) Partial loss of climate control systems

(2) Interruption of IS operations. This is loss of IS assets for an extended period of time that represent a significant impact on command mission accomplishment. System interruptions may result from:

(a) Failure of a major IS hardware unit
(b) Prolonged power interruption
(c) Fire, natural disaster or sabotage in the IS operations environment
(d) Corruption of system software

(3) Major destruction, disruption or damage to the IS facility and/or magnetic media. This is total loss of the IS facility or IS systems that represents a complete disruption of IS system operations. Causes may include:

(a) Catastrophic natural disaster
(b) Fire, flood or hostile action
(c) Permanent mechanical breakdown of IS hardware or software or climate control systems

5. Action

a. A command contingency planning team, consisting of the Executive Officer, System Administrator (SYSAD), Information Systems Security Officer (ISSO), Department Heads, and the Physical Security Officer will be responsible for contingency planning, coordination, periodic testing and implementation of this contingency plan in the event of an unexpected IS service interruption or significant service disruption.

b. The contingency planning team will evaluate IS vulnerabilities with respect to the current IS environment and establish specific loss-control measures. These loss-control measures will identify risks, define appropriate countermeasures and assign responsibilities to minimize the impact on mission operations.

c. In many cases there will be sufficient time to implement loss-control measures; however, in certain situations, safety of personnel may dictate immediate evacuation. Personal safety is of paramount concern and will not be jeopardized in the implementation of loss-control measures.

6. Agreements. Signatures acknowledge concurrence to this letter. Any changes to this plan will be considered an amendment and will require review, recommendations and concurrence.

T. D. BODE

Distribution:
NAVCRUITDISTPORTLANDINST 5216.1U
List A, B, C, and D

NAVY RECRUITING DISTRICT, PORTLAND
INFORMATION SYSTEMS (IS) CONTINGENCY PLAN

1. This contingency plan establishes procedures and outlines responsibilities to accomplish limited mission functions in the event of an unexpected service interruption that degrades NRD Portland LAN operations and/or availability. A backup procedure for software assets and limited duplication of hardware resources is the single most important element in establishing an effective loss-control program. Through effective restoration planning and well-defined contingency actions, continued IS mission critical operations are possible with only limited systems degradation. System restoration actions may take place on-site or may require relocation to an alternate site. This decision is based on resource availability, the scope of the disruption and operational need to preserve data confidentiality, software support integrity, and service availability. The DAA, with advice from the NRD Portland IAO, will direct all NRD Portland LAN contingency relocation or restoration efforts. Specific restoration measures include:

a. Major destruction or damage to the IS facility. Complete loss of operations as a result of major destruction to the IS facility or IS media assets caused by fire or natural disasters, such as earthquakes or floods, fire (including smoke and water damage resulting from fire), catastrophic loss of climate control systems or support equipment, or hostile action including sabotage.

(1) Hardware. Complete off-site duplication of command hardware assets to provide for uninterrupted operations following a major disruption of IS operations is not feasible. Therefore, contingency relocation options will be instituted which represent an acceptable level of mission degradation.

(a) Primary relocation procedures. In the event of a complete disruption of IS operating systems, selected NRD personnel may be relocated to NOSC Portland. Onboard systems and ancillary/peripheral equipment may be sufficient to provide mission-critical software-support services. This configuration represents a significant loss of total mission capability but may be sufficient to provide critical IS services in support of limited operations. Enclosure (2) provides an on-going Memorandum of Understanding between the commands involved.

(b) Alternate relocation procedures. Primary relocation is normally NOSC Portland. Local Navy recruiting stations (NRSs) and the Navy Liaison Office at Military Entrance and Processing Station (MEPS), Portland, may serve as alternate relocation sites, in the case where the primary location is not attainable for full support. NRD Seattle would be considered as a tertiary relocation site in the event that no local facility proved tenable (e.g., in the event of widespread damage in the Portland area). Full implementation of alternate relocation procedures will depend upon the availability of suitable hardware resources and work space. Relocation will require close coordination between the contingency planning team and alternate site representatives. Transfer of command personnel and resources to support alternate site relocation will be limited to only those necessary to achieve an acceptable level of operations.

(2) Software. Software redundancy is a key element in system contingency planning and service restoration management. Contingency software backups must reflect the most current version and be immediately accessible.

(a) Primary software backup. System and application software backup is the sole responsibility of NMCI. NMCI will be contacted in the event software is needed for reload to any NMCI assets. This will serve as the primary backup in the event of a catastrophic NRD Portland LAN software interruption. A call to the NMCI Helpdesk, 866-843-6624, for software restoration assistance is recommended, in conjunction with liaison with the Commander, Navy Recruiting Command Systems Administrator.

b. Interruption of IS operations. IS interruptions represent a significant degradation to command mission capability, but may not result in the complete loss of system services. System interruptions may result from primary hardware failure, corruption of system software, prolonged power interruption, localized fire damage or complications resulting from a natural disaster or hostile action.

(1) Hardware. Spare IS hardware assets are available to replace individual hardware assets or network peripheral or ancillary equipment. In the event of the failure

or loss of a significant number of hardware assets, the contingency planning team will assess the operational impact, determine the extent and expected duration of the outage and recommend a suitable course of action to the commanding officer.

(a) Primary restoration procedures. Command IS hardware assets are the primary source of replacement equipment to restore systems to an acceptable level of operation. Hardware limitations which may affect system operations will be analyzed by the contingency planning team and recommendations will be provided to the commanding officer.

(b) Alternate restoration procedures. In the event command hardware assets are unable to support an acceptable level of operations, alternate restoration procedures may require relocation of system operations to the primary relocation site or temporary disruption of operations pending system maintenance or hardware equipment acquisition. The contingency response will be based on the extent of the repairs needed, the time required to restore operations to an acceptable level, and the impact on overall mission requirements.

(2) Software. Locally duplicated software will be used in the event system relocation is required. Currently, NRD Portland is on the NMCI network and, therefore, does not require local backups, as NMCI technicians backup all NMCI servers on which command data is located. Software reflecting current operating versions may be downloaded from NMCI websites accessible by the NRD SYSAD. All mission critical applications may be restored through these resources.

(a) Primary restoration procedures. Use NMCI web-based tools to download software applications to users' new assets.

c. Limited loss of IS capability. An acceptable period of time for interruption or degradation of IS equipment will be based on the impact on overall mission requirements. System interruptions may occur as a result of peripheral equipment outage, power fluctuations or temporary power loss, system software failure or disruption of climate control equipment. In most cases, limited loss of IS equipment will not severely

impact command mission performance. The contingency planning team will keep the commanding officer apprised of all efforts to restore full system operations.

(1) Hardware

(a) Primary restoration procedures. Command IS hardware assets will be used to reduce or eliminate a limited loss of IS operational capability. Faulty IS equipment that causes an outage will be repaired by local and/or contract maintenance or replaced as necessary to restore full operations.

(b) Alternate restoration procedures. Interim use of hardware assets acquired from other compatible IS facilities may be required to maintain an acceptable level of operations. Additional alternatives may include system operation in a degraded mode or temporary interruption of system operations.

(2) Software. Software redundancy is a key element in system contingency planning and service restoration management. Contingency software backups must reflect the most current version and be immediately accessible.

(a) Primary restoration procedures. Use NMCI web-based tools to download software applications to users' new assets.

d. Testing and Evaluation. Periodic testing and evaluation is a critical aspect of successful contingency planning. The contingency planning team will test and evaluate backup and contingency relocation procedures identified in this contingency plan at least semi-annually. Tests will be broad in scope and be conducted around specific contingency scenarios. The results of each test will be documented and contain an overall assessment of the test results, an evaluation of the backup procedures used and recommendations to enhance command contingency procedures.

e. Network requirements. NRD headquarters will require NMCI network access with the following minimum equipment to complete its mission.

(1) Ten computers with Microsoft Office (will be provided by NMCI via the helpdesk).

(2) Five Mobile Recruiting Initiative (MRI) laptops (for temporary use until receipt of NMCI computers). These will be reallocated from local NRSs.

(3) One fax machine

(4) One copier

(5) 24/7 access to a facility

2. The contingency plan for the MEPS will depend on the direction of the MEPS Emergency Management and Assistance Plans (EMAP). Copies of these plans will be kept by the headquarters ISSO; a copy can also be obtained at each MEPS. Navy liaison personnel, in preparing for and responding to a major incident or condition that could severely impede ability to conduct operations, will be diverted as follows:

a. Navy Recruiting Processing Station (NRPS) Portland will relocate to the NRD Headquarters.

b. NRPS Boise will relocate to the nearest and most suitable NRS based upon the circumstances.

c. Applicants will be routed and accompanied as required in accordance with the EMAP for their location.

3. In the case of an incident occurring at an NRS, station personnel will relocate to the nearest NRS or district headquarters.

NAVCRUITDISTPORTLANDINST 5239.2B
16 Dec 13

Memorandum of Understanding

Between

Navy Recruiting District Portland

And

Navy Operational Support Center Portland

1. Purpose. To temporarily relocate to Navy Operational Support Center Portland in the event NRD Portland is unable to continue operations, at 7028 NE 79th Ct, Portland OR, 97218-2813.

2. Authority. By direction of CDR Todd D. Bode, Commanding Officer, Navy Recruiting District Portland, USN, and LCDR Heath Epaloose, Commanding Officer, Navy Operational Support Center Portland.

3. Implementation of Agreement. It is understood by all parties that if NRD Portland is no longer able to function in its current location, NRD Portland personnel will relocate, temporarily, to Navy Operational Support Center Portland. It is noted that there will be minimal information system support or availability, and limited space available for all personnel. Relocation will be limited to critical personnel, with an effort to relocate personnel where possible to outlying recruiting stations.

4. Effective Date. This MOU is effective upon signature of the parties named in this memorandum.

Todd D. Bode, CDR, USN
Commanding Officer
Navy Recruiting District Portland

Heath Epaloose, LCDR, USN
Commanding Officer
Navy Operational Support Center, Portland