



DEPARTMENT OF THE NAVY
NAVY RECRUITING DISTRICT, NEW ORLEANS
400 RUSSELL AVE BLDG 192
NEW ORLEANS, LOUISIANA 70143-5077

NAVCRUITDISTNOLAINST 5239.2D
40
6 Oct 2014

NAVCRUITDISTRICT NEW ORLEANS INSTRUCTION 5239.2D

From: Commanding Officer, Navy Recruiting District New Orleans

Subj: NAVY RECRUITING DISTRICT INFORMATION SYSTEMS (IS)
CONTINGENCY PLAN

Ref: (a) DoDD Directive 8500.01E
(b) SECNAVINST 5239.3B
(c) OPNAVINST 5239.1C
(d) COMNAVCRUITCOMINST 5239.3

1. Purpose. To establish Navy Recruiting District New Orleans' Information System (IS) Contingency Plan.
2. Cancellation. NAVCRUITDISTINST 5239.2C.
3. Background. As delineated in references (a) through (c) and as directed by reference (d) each Department of the Navy (DON) activity depends upon IS system operation to develop a contingency plan for IS systems and networks for which an unplanned disruption of service would have a critical impact on mission accomplishment.
4. Scope. This plan provides centralized guidance and identifies contingency measures that will be implemented in the event of an unforeseen LAN service interruption. The policies and procedures outlined in this Contingency Plan focus on the restoration of critical information services provided by the NRD LAN. Restoration and evaluation processes outlined in this Contingency Plan may be applied to other MEPS Information Systems and networks that are considered mission critical.
5. Policy. The establishment of an effective, well defined IS Contingency Plan is an integral part of the commands overall IS security posture. Special emphasis will be placed on personnel actions and hardware/software resources necessary to preserve mission integrity in the event of an unplanned IS service interruption. Specific IS contingency measures will address:

a. Limited Loss of IS Capability. Loss of IS capabilities for only a limited period of time with little or no operational impact. Risks include:

- (1) Failure of peripheral hardware.
- (2) Temporary power interruptions.
- (3) Partial loss of climate control systems.

b. Interruption of IS operation. Loss of IS assets for an extended period of time that represent a significant impact on command mission accomplishment. System interruptions may result from:

- (1) Failure of a major IS hardware unit.
- (2) Prolonged power interruption.
- (3) Fire, natural disaster or sabotage in the IS operations environment.
- (4) Corruption of system software.

c. Major Destruction, Disruption or Damage to the IS Facility and/or Magnetic Media. Total loss of the IS facility or IS systems that represent a complete disruption of IS system operations. Causes may include:

- (1) Catastrophic natural disaster.
- (2) Fire, flood or hostile action.
- (3) Permanent mechanical breakdown of IS system hardware or software or climate control systems.

6. Procedures. The IS Contingency Procedures provide specific procedures necessary to reduce or eliminate the operation impact of a LAN system interruption. A Command Contingency Planning Team, consisting of the Command Security Manager, Systems Administrator (SYSAD), Department Heads, and Physical Security Officer will be responsible for contingency planning,

coordination, periodic testing and the implementation of this Contingency Plan in the event of an unexpected LAN service interruption or significant service disruption. In fulfilling these responsibilities the Contingency Planning Team will evaluate system and network 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 command IS mission operations. In many cases there will be sufficient time to implement loss control measures, however, in certain situations personnel safety may dictate immediate evacuation. Personnel safety is of paramount concern and will not be jeopardized in the implementation of loss control measures. This Contingency Plan will be reviewed annually and updated as required.

7. Recruiting Field Activities Disaster Recovery Plan

a. Each Navy Recruiting Station (NRS) under NRD New Orleans will have the following Contingency Plan:

(1) When a NRS loses its ability to remotely connect to Commander, Navy Recruiting Command (CNRC) due to any foreign uncontrollable force, and it is anticipated that service shall not be regained within 24 hours, it's Division Officer (DIVO) shall immediately notify the SYSAD and relocate all station personnel to the nearest NRS and continue to perform all processing procedures using that station's phone lines and internet connection until service or other arrangements are made to restore its original station phone line and internet connection.

b. Each Navy Recruit Processing Station (NRPS) under NRD NOLA will have the following Contingency Plan:

(2) When NRPS New Orleans loses its LAN connection through MEPSCOM due to any foreign uncontrollable force, and it is anticipated that service shall not be regained within 24 hours, New Orleans' EPDS shall immediately contact SYSAD and relocate key personnel to NAS, JRB New Orleans bldg 192, and continue to perform all processing procedures using either Headquarters LAN system or air card connections until service or other arrangements are made for MEPS NOLA to restore its

original LAN connection. However, should the area of New Orleans lose all connections due to foreign uncontrollable forces, and it is anticipated that service shall not be regained within 24 hours, NRPS New Orleans shall notify SYSAD and relocate key personnel to NRS Meridian and continue to perform all processing procedures until service or other arrangements are made to restore New Orleans to its original LAN connection. Applicants will be diverted to the nearest MEPS, some to MEPS Jackson, MS and other to MEPS Shreveport, LA.

8. NRD Headquarters LAN Contingency Procedures. This contingency plan establishes procedures and outlines responsibilities to accomplish limited mission functions in the event of an unexpected service interruption contingency that degrades NRD LAN operations and/or availability. Backup procedures 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 system degradation. System restoration actions may take place on-site or may require relocation to an alternate site. This decision must be based on resource availability, scope of the contingency and operational need to preserve data confidentiality, software support integrity and service availability. The CO, with advice from the SYSAD, will direct all NRD LAN contingency relocations or restorations efforts. Specific restoration control 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, router, server and/or IS media assets caused by natural disasters; such as hurricanes, tornadoes or floods; fire including smoke and water damage resultant from fire; catastrophic loss of climate control systems or support equipment, and to a lesser extent, hostile action including sabotage.

(1) Hardware. Complete off site duplication of command LAN 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, all SYSAD operators and technicians will be relocated to Meridian 1183 Bonita Lakes Circle, Ste. A, Meridian, MS. 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 some tactical operations. The personnel to be relocated are the command section (CO and XO), the operations section (ROPS, AOPS, CR, and ACRs), and the IT Department (SYSAD and ASYSAD). All government assigned cell phones must be brought with relocating personnel at a minimum. If possible government supplied laptops, or desktop computers will be relocated along with personnel. The XO will have coordinated with SYSAD a relocation station to arrange actual space and internet connectivity. Spare computers and a printer should be in the agreement.

(b) Alternate Relocation Procedures. The Saufley Pensacola, Fl station may serve as the alternate relocation site, in the case where the primary location is not attainable, for NRD NOLA LAN support. Full implementation of alternate relocation procedures will depend upon the availability suitable hardware resources and processing time. 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 that 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.

(3) Primary Software Backup. System and application software backups will be stored at Buildings 192, NAS, JRB New Orleans, LA. These stored software assets will serve as the primary backups in the event of a catastrophic NRD NOLA LAN software interruption. Secure containers for duplicated software will be controlled and maintained by the Systems Administrator (SYSAD) Department.

Access to these containers will be limited to only those who are properly cleared and have an operational need to access the material. Detailed procedures regarding backups/restorations are contained in the SYSAD Department, SOP manual.

b. Interruption of IS Operations. NRD NOLA LAN interruptions represent a significant degradation in command IS 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 resultant from a natural disaster or hostile action.

(1) Hardware. Sufficient IS hardware assets are currently available to meet NRD NOLA LAN system or network interruptions affecting an individual hardware asset or single network peripheral or ancillary equipment. In the event of the failure or loss of a significant number of NRD NOLA 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 the LAN to a full or acceptable level of operation. System restoration procedures have been designed to reduce or eliminate the impact on overall command mission performance. Hardware limitations which may affect system operations, will be analyzed by the Contingency Planning Team and recommendations provided to the Commanding Officer.

(b) Alternate Restoration Procedures. In the event command hardware assets are unable to support an acceptable level of NRD NOLA LAN performance, 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. The NMCI network maintains backup of software which is accessible via internet connection.

(a) Primary Restoration Procedures. Locally controlled copies of system and application software will be used to restore operations following a software related service interruption.

(b) Alternate Restoration Procedures. Software assets stored at NAS, JRB New Orleans, Bldg 192, will be used in the event command software backups are rendered unusable. Other fleet operational sites may serve as an additional source for acquiring the current operating version of system and application software or database information.

c. Limited Loss of IS Capability. Interruption or degradation of NRD NOLA Virtual Private Network (VPN) operation for an acceptable period of time will be based on the extent of system operations and impact on overall mission requirements. System interruptions may occur as a result of peripheral equipment outage, power fluctuations or temporary loss, system software failure and disruption of climate control equipment. In most cases limited loss of NRD NOLA capability 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 NRD NOLA VPN operational capability. IS equipment effecting VPN or network 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 Recruit Servicing Network (RSN) or any other compatible IS facility may be required to maintain an acceptable level of operations. Additional alternatives may include system operation in a degraded mode, a periods processing mode or temporary interruption of system operations.

(2) Software

(a) Primary Restoration Procedures. Duplicate copies of NRD NOLA LAN system, application, utility and applicable database software retained within the command will serve as primary back up in the event of a software failure.

(b) Alternate Restoration Procedures. Command software assets retained at NAS, JRB New Orleans, Bldg 192, will be used as alternate software backups.

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 annually. Tests will be broad in scope and be conducted around a specific contingency scenario. The results of each test will be documented and contain a description of the scenario, an overall assessment of the test results, an evaluation of the backup procedures used and any recommendations to enhance command contingency procedures.

/s/
C. A. STOVER

Distribution List:
Electronic only, via
<http://www.cnrc.navy.mil/neworleans>