

DON CIO Message: DTG: 291600Z FEB 08
UNCLASSIFIED//

SUBJ/DEPARTMENT OF THE NAVY (DON) CONTINGENCY PLANS AND TESTING
GUIDANCE//

REF/A/DOC/FISMA/23JAN2002//
REF/B/DOC/DODIG/05FEB2008//
REF/C/DOC/DON/MAR2006//
REF/D/DOC/DOD/28NOV2007//
REF/E/DOC/DOD/06FEB2003//
REF/F/DOC/DON/13JUN2007//

NARR/REF A, FEDERAL INFORMATION SECURITY MANAGEMENT ACT (FISMA), PROVIDES THE REQUIREMENT FOR EACH FEDERAL AGENCY TO ESTABLISH AND MAINTAIN COMPLIANT INFORMATION SECURITY PROGRAMS. REF B, DOD OFFICE OF THE INSPECTOR GENERAL (DOD IG) AUDIT REPORT CONTINGENCY PLANNING FOR DOD MISSION-CRITICAL INFORMATION SYSTEMS D-2008-047, LOCATED ON THE DOD IG WEB SITE (www.dodig.mil/Audit/reports/index.html), DISCUSSES DEFICIENCIES IN CURRENT DOD AND DON PROCESSES AND POLICIES REGARDING CONTINGENCY PLANS AND EXERCISES. REF C, DON FISMA GUIDANCE OF MARCH 2006, LOCATED ON THE DON CIO AND NAVY INFOSEC WEB SITES, PROVIDES THE DON SECURITY PLAN OF ACTION AND MILESTONES (POA&M) GUIDANCE. REF D, THE DOD INFORMATION ASSURANCE CERTIFICATION AND ACCREDITATION PROCESS (DIACAP) INSTRUCTION 8510.01, PROVIDES THE DOD CERTIFICATION AND ACCREDITATION PROCESS REQUIREMENTS. REF E IS THE DOD INFORMATION ASSURANCE IMPLEMENTATION INSTRUCTION 8500.2. REF F IS THE DON FISMA REPORTING RESPONSIBILITIES FOR FY2007.//

POC/RICHARD ETTER/CIVPERS/DON CIO/LOC: WASHINGTON DC/TEL: 703-602-6882/EMAIL: RICHARD.ETTER@NAVY.MIL//

POC/JAMES COLLINS/CTR/DON CIO/LOC: WASHINGTON DC/TEL:703-602-6202/
EMAIL: JAMES.E.COLLINS.CTR@NAVY.MIL//

POC/JENNIFER ELLETT/CTR/DON CIO/LOC: WASHINGTON DC/TEL:703-602-6110/EMAIL: JENNIFER.ELLETT.CTR@NAVY.MIL

POC/CHARLES BUCKLEY/CAPT/HQMC C4/LOC: WASHINGTON DC/TEL: 703-693-490/
EMAIL: CHARLES.BUCKLEY@USMC.MIL//

POC/STU WHARTON/CDR/OPNAV N6131/LOC: WASHINGTON DC/TEL: (703) 604-7736
/EMAIL: STEWART.WHARTON@NAVY.MIL //

POC/TONY PLATER/CTR/OPNAV N61/LOC: WASHINGTON DC/TEL: 703-601-1367/EMAIL:ALVIN.PLATER.CTR@NAVY.MIL//

CNO: PLEASE PASS TO DNS/N091/N093/N095/N097/N1/N2/N3/N5/N4/N6/N8//

NAVY ECHELON 2 COMMANDS: PLEASE PASS TO COMMAND INFORMATION OFFICER (IO)/N6

USMC MAJOR SUBORDINATE COMMANDS: PLEASE PASS TO COMMAND INFORMATION OFFICER (IO)/G1/G6//

RMKS/1. THIS MESSAGE PROVIDES DEPARTMENT OF THE NAVY (DON) REQUIREMENTS FOR RESOLVING DEFICIENCIES IN CONTINGENCY PLANNING

IDENTIFIED BY THE DEPARTMENT OF DEFENSE INSPECTOR GENERAL (DOD IG) AUDIT, REF B, AND ENSURING DON POLICY ALIGNS WITH INFORMATION ASSURANCE (IA) REQUIREMENTS IN REFS A, C, D, AND E.

2. BACKGROUND: IN JANUARY 2007, THE DOD IG PULLED SAMPLING DATA FROM THE DEPARTMENT OF DEFENSE (DOD) DEFENSE INFORMATION TECHNOLOGY PORTFOLIO REPOSITORY (DITPR) ON CONTINGENCY PLANS AND CONTINGENCY PLAN EXERCISE DATES FOR FISMA MISSION CRITICAL (MC) SYSTEMS. THE DON WAS REQUIRED, AS PART OF THE AUDIT, TO PROVIDE COPIES OF THE CONTINGENCY PLANS AND THE EXERCISE DOCUMENTATION FOR THE SYSTEMS SAMPLED. THE QUALITY OF INFORMATION FROM SYSTEM OWNERS WAS POOR. THE DEPARTMENT OF THE NAVY CHIEF INFORMATION OFFICER (DON CIO) HAS RECEIVED A SERIES OF RECOMMENDATIONS FROM THE DOD IG TO RESOLVE THE ISSUES IDENTIFIED IN THE AUDIT.

3. IN RESPONSE TO THE IG AUDIT, COMMANDS FORWARDED EITHER A CONTINGENCY PLAN OR A CONTINUITY OF OPERATIONS PLAN (COOP). THE TERMS ARE OFTEN USED INTERCHANGABLY IN CURRENT DOD AND DON FISMA REPORT GUIDANCE AND DOD DITPR GUIDANCE. A CONTINGENCY PLAN IS NOT SYNONIMOUS WITH A COOP. DETAILED DEFINITIONS OF CONTINGENCY PLAN AND COOP ARE FOUND IN NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST) SPECIAL PUBLICATION (SP) 800-34. IN SIMPLE TERMS, THE DEFINITIONS OF CONTINGENCY PLANS AND COOP MAY BE PARAPHRASED AS FOLLOWS:

A. A CONTINGENCY PLANS DESCRIBES THE INTERIM MEASURES USED TO RECOVER AND RESTORE INFORMATION TECHNOLOGY SYSTEMS AND SERVICE OPERATIONS FOLLOWING AN EMERGENCY OR SYSTEM DISRUPTION.

B. A COOP DESCRIBES THE RESTORATION OF MISSION AND ORGANIZATIONAL OPERATIONS, WHICH MAY NOT ALWAYS INCLUDE THE RESTORATION OF AN INFORMATION SYSTEM.

4. ACTION.

A. AS OF THIS MESSAGE, AND TO BE INCORPORATED IN FUTURE DON POLICY, THE FOLLOWING REQUIREMENTS APPLY TO ALL CONTINGENCY PLANS:

(1) SYSTEM OWNERS MUST DEVELOP A CONTINGENCY PLAN FOR EVERY INFORMATION SYSTEM, TO BE MAINTAINED AFTER APPROVAL IN THE PROGRAM OFFICE. SYSTEM OWNERS ARE RESPONSIBLE FOR DEVELOPING A CONTINGENCY PLAN FOR THEIR SYSTEM EVEN IF THE SYSTEM IS NOT OPERATED BY THE SYSTEM OWNER (E.G., PROGRAMS OF RECORD AND TYPE ACCREDITED SYSTEMS).

(2) THE CONTINGENCY PLAN MUST PROVIDE SPECIFIC GUIDANCE TO THE SITE INFORMATION ASSURANCE MANAGER ON THE SYSTEM REQUIREMENTS FOR RECOVERY FROM A DISRUPTIVE EVENT OR EMERGENCY FOR INCORPORATION INTO THE SITE CONTINGENCY AND COOP PLANS.

(3) CONTINGENCY PLANS MUST ADHERE TO NIST SP 800-34, CONTINGENCY PLANNING GUIDE FOR INFORMATION TECHNOLOGY SYSTEMS, JUNE 2002.

(4) CONTINGENCY PLANS MUST NAME THE SYSTEM IN THE PLAN. THE SYSTEM NAME MUST MATCH WHAT IS REGISTERED IN THE DEFENSE INFORMATION TECHNOLOGY PORTFOLIO REPOSITORY ? DEPARTMENT OF NAVY (DITPR-DON), AND THE APPLICABLE CERTIFICATION & ACCREDITATION (C&A) DOCUMENTATION.

(5) THE USER REPRESENTATIVE, PROGRAM MANAGER, AND DESIGNATED ACCREDITING AUTHORITY (DAA) MUST ALL APPROVE AND SIGN CONTINGENCY PLANS. REF D DEFINES USER REPRESENTATIVES AS AN INDIVIDUAL OR ORGANIZATION THAT REPRESENTS THE USER COMMUNITY FOR A PARTICULAR SYSTEM FOR DEFENSE INFORMATION ASSURANCE CERTIFICATION AND ACCREDITATION PROCESS (DIACAP) PURPOSES. A SEPARATE CONTINGENCY PLAN SIGNATURE PAGE IS REQUIRED AND MUST BE MAINTAINED WITH THE CONTINGENCY PLAN. A CONTINGENCY PLAN WILL NOT BE CONSIDERED VALID WITHOUT ALL THREE SIGNATURES.

(6) THE DAA IS REQUIRED, AS THE FINAL REVIEW AND APPROVAL FOR CONTINGENCY PLANS, TO REPORT CONTINGENCY PLAN STATUS INTO DITPR-DON WHEN A SYSTEM ACCREDITATION STATEMENT IS ISSUED.

B. CONTINGENCY PLAN EXERCISE REQUIREMENTS:

(1) CONTINGENCY PLANS SHALL BE EXERCISED IN ACCORDANCE WITH REF E, I.E., AT LEAST TWICE EVERY 12 MONTHS FOR MISSION ASSURANCE CATEGORY (MAC) I SYSTEMS, AND AT LEAST ONCE EVERY 12 MONTHS FOR MAC II AND MAC III SYSTEMS.

(2) EXERCISES MUST BE REALISTIC AND TESTED IN ACCORDANCE WITH REFS E AND F. REAL WORLD EVENTS (HARDWARE FAILURES, POWER OUTAGES, ETC.) MAY BE DOCUMENTED AS PART OF THE PLAN REVIEW PROCESS, BUT IN ORDER TO ENSURE ALL ASPECTS OF CONTINGENCY PLANS ARE EXERCISED, THOSE PARTS OF THE CONTINGENCY PLAN THAT HAVE NOT BEEN ADDRESSED IN REAL WORLD EVENTS MUST STILL BE TESTED.

(3) EXERCISES MUST BE DOCUMENTED, SIGNED, AND DATED. DOCUMENTATION MUST INCLUDE THE NAME OF THE SYSTEM AND MUST SPECIFICALLY STATE WHAT WAS TESTED AND HOW. COOP CHECKLISTS DO NOT QUALIFY AS DOCUMENTATION FOR CONTINGENCY PLAN EXERCISES.

(4) SINCE THE CONTINGENCY PLAN EXERCISE IS PART OF THE ACCREDITATION PROCESS, THE DAA WILL ENTER THE INITIAL CONTINGENCY PLAN EXERCISE DATE IN DITPR-DON FOR A NEW ACCREDITATION. IN SUBSEQUENT YEARS, PROGRAM MANAGERS ARE RESPONSIBLE FOR ENSURING THE UPDATED CONTINGENCY PLAN EXERCISE DATE IS ENTERED IN DITPR-DON. THE DAA, AS PART OF THE DIACAP ANNUAL REVIEW, WILL AUDIT AND VALIDATE SYSTEM CONTINGENCY PLAN RELATED DATA IN DITPR-DON TO ENSURE IT IS COMPLETE, ACCURATE, AND MATCHES SYSTEM DOCUMENTATION.

C. FOR ALL SYSTEMS IDENTIFIED AS DEFICIENT IN THE DOD IG AUDIT REPORT (REF B), SYSTEM OWNERS ARE REQUIRED TO CREATE A SECURITY POA&M OR ADD ENTRIES TO AN EXISTING POA&M DOCUMENTING THE DEFICIENCIES AND PLANNED RESOLUTION. POA&MS MUST BE SUBMITTED TO THE COMMAND INFORMATION OFFICER (IO) FOR REVIEW, ACCEPTANCE, CONSOLIDATION, AND RETENTION. THE POA&M MUST ALSO BE PROVIDED TO THE OPERATIONAL DAA FOR VALIDATION AND APPROVAL. THE OPERATIONAL DAA APPROVED POA&M DOCUMENTING DEFICIENCIES IDENTIFIED IN THIS AUDIT MUST BE SUBMITTED TO THE DON CIO NLT 60 DAYS FROM THE DATE THE AUDIT REPORT WAS ISSUED (05 FEBRUARY 2008).

D. WITHIN 180 DAYS OF THE ISSUANCE OF THIS MESSAGE THE SERVICES SHALL REQUIRE COMMAND IOS COMPLETE A ONE TIME DATA QUALITY AUDIT OF ALL DITPR-DON REGISTERED SYSTEMS FOR WHICH THE C&A REQUIRED ANSWER IS ?YES.? THE FOLLOWING REQUIREMENTS APPLY TO THIS AUDIT:

(1) EVERY SYSTEM SHALL BE AUDITED FOR ACCURATE REPORTING OF CONTINGENCY PLAN AND CONTINGENCY PLAN EXERCISE DATE. COMMAND IOS MUST AUDIT SIGNED DOCUMENTATION TO ENSURE IT MATCHES THE DATA BEING REPORTED IN DITPR-DON.

(2) COMMAND IOS MUST REVIEW DOCUMENTATION FOR CP AND EXERCISES TO ENSURE IT MEETS THE DON REQUIREMENTS STATED IN THIS MESSAGE.

E. COMMAND IOS SHALL AUDIT MC AND MAC LEVELS REPORTED IN DITPR-DON AGAINST DOCUMENTATION SIGNED BY THE MILESTONE DECISION AUTHORITY STATING THE MC AND MAC DESIGNATED LEVELS. SYSTEMS IDENTIFIED FOR THE AUDIT WERE ALL LISTED IN DITPR AS MISSION CRITICAL SYSTEMS. BY DEFINITION, THE LOSS OF OPERATION OF A MISSION-CRITICAL SYSTEM WILL CAUSE THE STOPPAGE OF WARFIGHTER OPERATIONS.

F. FOR ALL SYSTEMS DESIGNATED AS MC AND MAC III, REVIEW RATIONALE FOR THE DESIGNATIONS. RATIONAL MUST BE DOCUMENTED IN THE SYSTEM SECURITY CERTIFICATION AND ACCREDITATION DOCUMENTATION.

G. COMMAND IOS SHALL DOCUMENT THEIR AUDIT EVALUATIONS AND ANY ISSUES DISCOVERED, AND REPORT COMPLETION OF THEIR AUDITS TO THE DON DEPUTY CIO (NAVY OR MARINE CORPS). THE DON DEPUTY CIO (NAVY AND MARINE CORPS) REPORT COMPLETION OF AUDITS TO THE DON CIO BY THE END OF FY 2008.

H. FOR EACH SYSTEM IDENTIFIED IN THE ABOVE AUDITS AS HAVING A DATA QUALITY ISSUE IN DITPR-DON, THE SYSTEM OWNER IS REQUIRED TO CREATE A SECURITY POA&M OR ADD ENTRIES TO EXISTING POA&MS DOCUMENTING THE DEFICIENCY AND PLANNED RESOLUTION. POA&MS WILL BE SUBMITTED TO THE COMMAND IO AND OPERATIONAL DAA FOR APPROVAL.

5. RELEASED BY ROBERT J. CAREY, DEPARTMENT OF THE NAVY CHIEF INFORMATION OFFICER.//