

UNCLASSIFIED//

PRECEDENCE TO: ROUTINE DTG: 051610Z NOV 09  
PRECEDENCE CC: ROUTINE  
TYPE: DMS SIGNED/ENCRYPTED  
FROM PLA: DON CIO WASHINGTON DC

ORIGINAL TO RECIPIENTS:

TO CNO N6  
CMC C4  
AAUSN//  
COMUSFLTFORCOM NORFOLK VA//  
COMUSNAVEUR NAPLES IT//  
COMPACFLT PEARL HARBOR HI//  
USNA ANNAPOLIS MD//  
COMUSNAVCENT BAHRAIN//  
COMNAVRESFORCOM NORFOLK VA//  
COMNAVAIRSYS COM PATUXENT RIVER MD///  
BUMED WASHINGTON DC//  
NETC PENSACOLA FL//  
COMNAVSEASYS COM WASHINGTON DC//  
FLDSUPPACT WASHINGTON DC//  
COMNAV SUPSYS COM MECHANICSBURG PA//  
DIRSSP WASHINGTON DC//  
CNIC WASHINGTON DC//  
COMNAVLEGSVCCOM WASHINGTON DC//  
NAVPGSCOL MONTEREY CA//  
COMNAV FACENG COM WASHINGTON DC//  
COMNAVSAFECEN NORFOLK VA//  
BUPERS MILLINGTON TN//  
NAVWARCOL NEWPORT RI//  
ONI WASHINGTON DC//  
COMNAV SPECWARCOM CORONDAO CA//  
COM SPAWAR SYS COM SAN DIEGO CA//  
COMNAV DIST WASHINGTON DC//  
NAV HISTHERITAGE COM WASHINGTON DC//  
COM MARCORSYS COM QUANTICO VA//  
COM MARFOREUR//  
COM MARFORCOM//  
COM MARFORPAC//  
COM MARFORRES//  
COM MARFORSOUTH//  
COM MARSOC//  
CG MCCDC QUANTICO VA//  
CG MCRC//  
CG TECOM//  
COMNAVNETWARCOM NORFOLK VA//

UNCLASSIFIED//

MSGID/GENADMIN/DON CIO WASHINGTON DC//

SUBJ/DEPARTMENT OF THE NAVY FEDERAL INFORMATION SECURITY MANAGEMENT ACT  
GOALS FOR FY 2010//

REF/A/DOC/23JAN2002//

REF/B/DOC/JUNE2006//

REF/C/DOC/28NOV07/  
REF/D/DOC/29SEP2009//

NARR/REF A, FEDERAL INFORMATION SECURITY MANAGEMENT ACT OF 2002 (FISMA), PROVIDES THE REQUIREMENT FOR EACH FEDERAL AGENCY TO ESTABLISH AND MAINTAIN COMPLIANT INFORMATION SECURITY PROGRAMS. REF B, DOD INFORMATION TECHNOLOGY PORTFOLIO REPOSITORY DEPARTMENT OF THE NAVY (DITPR-DON) REGISTRATION GUIDANCE FOR 2006, LOCATED ON THE DON CIO WEB SITE ([WWW.DONCIO.NAVY.MIL](http://WWW.DONCIO.NAVY.MIL)), PROVIDES CURRENT REQUIREMENTS FOR REGISTERING SYSTEMS IN DITPR-DON. REF C, DOD INFORMATION ASSURANCE CERTIFICATION AND ACCREDITATION PROCESS (DIACAP) INSTRUCTION, PROVIDES REQUIREMENTS FOR EVALUATING SECURITY OF SYSTEMS. REF D, DON IT POLICY GUIDANCE FOR FY2010, REQUIRES SYSTEMS NOT IN COMPLIANCE WITH FISMA REQUIREMENTS EACH QUARTER TO EXPEND DEVELOPMENT/ MODERNIZATION FUNDS ONLY ON ACTIONS NECESSARY TO OBTAIN COMPLIANCE WITH FISMA.//

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

POC/JENNIFER ELLETT/CTR/DON CIO/LOC: WASHINGTON DC/TEL:703-602-6759/EMAIL: JENNIFER.ELLETT.CTR@NAVY.MIL//

POC/RAY LETTEER/CIV/HQMC C4/: WASHINGTON DC/TEL:703-693-3490/EMAIL: RAY.LETTEER@USMC.MIL//

POC/JOHN ROSS/CIV/OPNAV N6133/LOC: WASHINGTON DC/TEL: 703-604-7736/EMAIL: JOHN.R.ROSS@NAVY.MIL//

POC/WILL MCKNIGHT/CTR/OPNAV N6133B/LOC: WASHINGTON DC/TEL: 703-604-703/EMAIL: WILFRED.MCKNIGHT.CTR@NAVY.MIL//

CNO: PLEASE PASS TO N6

NAVY ECHELON II COMMANDS: PLEASE PASS TO COMMAND INFORMATION OFFICER(IO), N6 AND OTHERS DEEMED APPROPRIATE//

USMC MAJOR SUBORDINATE COMMANDS: PLEASE PASS TO COMMAND INFORMATION OFFICER (IO), G1, G6 AND OTHERS DEEMED APPROPRIATE//

RMKS/1. THIS MESSAGE PROVIDES DEPARTMENT OF THE NAVY (DON) FEDERAL INFORMATION SECURITY MANAGEMENT ACT (FISMA) GOALS FOR FY10, INCLUDING QUARTERLY REPORTING REQUIREMENTS.

2. BACKGROUND: FISMA (REF A) REQUIRES THAT EACH FEDERAL AGENCY REPORT A SUMMARY STATUS OF INFORMATION TECHNOLOGY (IT) SYSTEM SECURITY TO THE OFFICE OF MANAGEMENT AND BUDGET (OMB) ANNUALLY. OMB REPORTS THESE RESULTS TO CONGRESS ANNUALLY FOR ASSESSMENT AND GRADING OF THE STATE OF INFORMATION SECURITY WITHIN EACH FEDERAL AGENCY. IT IS CRITICAL THAT ALL NAVY AND MARINE CORPS SYSTEMS ARE IN FULL COMPLIANCE WITH THE FISMA REPORTING REQUIREMENTS AT ALL TIMES. THE DON IS CLOSELY MONITORING THESE STATISTICS TO ENSURE COMPLIANCE WITH REQUIREMENTS IS CONTINUALLY MAINTAINED.

3. OMB IS NOT REQUIRING FISMA QUARTERLY REPORTING FOR FIRST QUARTER FY10, BUT THE DON CHIEF INFORMATION OFFICER (CIO) IS MAINTAINING THIS REQUIREMENT. IT IS ANTICIPATED THAT OMB WILL ISSUE NEW QUARTERLY REPORTING REQUIREMENTS FOR QUARTERS 2, 3, AND 4 TOWARD THE END OF THE

2009 CALENDAR YEAR. IT IS ALSO ANTICIPATED THAT OMB WILL ISSUE NEW 2010 ANNUAL FISMA REPORTING REQUIREMENTS, INCLUDING NEW MEANINGFUL METRICS TO ASSESS OUR CYBER SECURITY LATER THIS YEAR. WHEN THAT OCCURS, DON CIO WILL RELEASE A MESSAGE WITH THE NEW REPORTING REQUIREMENTS. HOWEVER, THE REQUIREMENTS STATED IN THIS MESSAGE SHOULD BE FOLLOWED UNTIL A NEW DON CIO MESSAGE ON UPDATED REPORTING REQUIREMENTS IS ISSUED.

4. ACTION FOR ALL DON:

A. IN ACCORDANCE WITH REF B, ALL ACTIVE MISSION CRITICAL (MC), MISSION ESSENTIAL (ME), AND MISSION SUPPORT (MS) SYSTEMS MUST BE REGISTERED IN DOD INFORMATION TECHNOLOGY PORTFOLIO REPOSITORY DEPARTMENT OF THE NAVY (DITPR-DON).

B. EACH COMMAND WITH IT ASSETS REQUIRING C&A MUST CONTINUE TO MAINTAIN 100 PERCENT ACCREDITATION (I.E., AUTHORIZATION TO OPERATE (ATO) OR INTERIM AUTHORIZATION TO OPERATE (IATO)) AT ALL TIMES.

C. ALL SYSTEMS WITH AN ACCREDITATION ARE REQUIRED TO DEVELOP AND MAINTAIN A PLAN OF ACTION AND MILESTONES (POA&M) DOCUMENTING CORRECTIVE ACTIONS FOR IDENTIFIED WEAKNESSES TO BE COMPLETED WITHIN THE AUTHORIZATION PERIOD. PER REF C, THESE POA&MS ARE TO BE SUBMITTED AND APPROVED BY THE RESPECTIVE OPERATIONAL/ENTERPRISE DESIGNATED ACCREDITING AUTHORITIES (DAA).

D. MAINTAIN 100 PERCENT COMPLIANCE AT ALL TIMES WITH THE FISMA-REQUIRED ANNUAL SECURITY REVIEWS, ANNUAL TESTING OF SECURITY CONTROLS, AND ANNUAL EVALUATION OF CONTINGENCY PLANS (CP). EACH SYSTEM MUST MAINTAIN COMPLIANCE WITH THE REQUIRED ANNUAL REVIEWS, TESTS, AND EVALUATIONS WITHIN THE TWELVE MONTH WINDOW OF THE LAST TEST. COMMANDS MUST COMPLETE TESTS BEFORE THE ANNUAL EXPIRATION DATE TO ENSURE NO SYSTEM FALLS OUT OF COMPLIANCE.

E. ENSURE MILESTONES LISTED IN A POA&M ARE ACHIEVABLE AND MET WITHIN THE TIMELINE CONTAINED IN THE POA&M. THE DAAS ARE RESPONSIBLE FOR MONITORING POA&M MILESTONES AND TRACKING COMPLIANCE. DAAS ARE RESPONSIBLE FOR REVIEWING ANY MISSED MILESTONES TO ENSURE THEY DO NOT NEGATIVELY IMPACT THE RISK ACCEPTANCE FOR THE SYSTEM.

5. CONSEQUENCES FOR NON-COMPLIANCE:

A. PER REF (D) IF ANY INDIVIDUAL FISMA-REPORTED SYSTEM (C&A REQUIRED QUALS "YES" IN DITPR-DON) IS REPORTED AS DELINQUENT ON ANY OF THE ANNUAL TESTS, EVALUATIONS, REVIEWS, ACCREDITATION, OR PRIVACY IMPACT ASSESSMENT REQUIREMENTS FOR FISMA QUARTERLY REPORTS, DEVELOPMENT/MODERNIZATION FUNDS MAY BE EXPENDED ONLY ON ACTIONS NECESSARY TO OBTAIN FISMA COMPLIANCE UNTIL COMPLIANCE IS ACHIEVED.

B. DON CIO WILL ASSESS COMPLIANCE QUARTERLY, BASED ONLY ON DITPR-DON REPORTED DATA ON OR ABOUT 13 NOV 2009, 18 FEB 2010, 20 MAY 2010, AND 19 AUG 2010.

C. SYSTEMS FOUND TO BE NON-COMPLIANT IN DITPR-DON AT ANY TIME MAY BE REVIEWED BY DON CIO FOR CONSEQUENCES IN ADDITION TO THE FUNDING RESTRICTIONS LISTED ABOVE, TO INCLUDE ISSUANCE OF A DENIAL OF AUTHORIZATION TO OPERATE (DATO). THE SECURITY OF DON SYSTEMS AND

NETWORKS IS TOP PRIORITY AND NON-COMPLIANCE WITH SECURITY REQUIREMENTS INTRODUCES ADDITIONAL RISK TO DON NETWORKS AND SYSTEMS. IF THE RISK IS DEEMED UNACCEPTABLE BECAUSE A SYSTEM IS NOT OPERATING SECURELY AND MEETING FISMA REQUIREMENTS, IT MAY BE DETERMINED THAT THE SYSTEM MUST BE REMOVED FROM THE NETWORK AND ISSUED A DATO.

6. POA&M QUARTERLY REPORTING REQUIREMENTS FOR ALL FISMA SYSTEMS:

A. SYSTEMS THAT ARE OPERATING WITH AN OPEN SECURITY WEAKNESS MUST INDICATE "YES" IN THE FISMA SCREEN FOR DITPR-DON DATA ELEMENT #10, "IS THERE A POA&M WITH AN OPEN WEAKNESS?"

B. FOR SYSTEMS OPERATING WITH AN OPEN WEAKNESS MORE THAN 90 DAYS PAST THE MILESTONE DATE, PROGRAM MANAGERS MUST INDICATE "YES" IN THE APPROPRIATE DITPR-DON QUESTION, EITHER 10A "GREATER THAN 120 DAYS BEYOND REMEDIATION DATE" OR 10B "90 TO 120 DAYS BEYOND REMEDIATION DATE."

C. DATA FROM POA&M QUESTIONS 10A AND 10B WILL BE COMPILED QUARTERLY ON THE DATES INDICATED IN PARAGRAPH 5B. THEREFORE, THE DATES CALCULATED FOR OPEN WEAKNESSES PAST THE MILESTONE DATE SHOULD BE BASED ON THE NEXT QUARTERLY REPORTING DATE.

D. FOR SYSTEMS MORE THAN 90 DAYS PAST A MILESTONE DATE WITH AN OPEN WEAKNESS, PROGRAM MANAGERS ALSO MUST PROVIDE THE APPROPRIATE DAA AND THE DON DEPUTY CIO (NAVY) OR DON DEPUTY CIO (MARINE CORPS) A WRITTEN EXECUTIVE SUMMARY PROVIDING SYSTEM NAME, MISSION ASSURANCE CATEGORY LEVEL, MISSED MILESTONE AND ITS DATE, AND NEW MILESTONE DATE FOR RESOLVING THE DEFICIENCY. THESE EXECUTIVE SUMMARIES WILL BE PROVIDED BY THE DON DEPUTIES TO THE DON SENIOR INFORMATION ASSURANCE OFFICER (SIAO) BY THE DATES LISTED IN PARAGRAPH 5B.

7. FOR INFORMATION, THE DON CIO WILL PROVIDE SEMI-MONTHLY STATUS UPDATES ON ATO RATES, UPCOMING ATO EXPIRATIONS, AND COMPLIANCE RATES FOR THE ANNUAL TESTS, REVIEWS, AND EVALUATION REQUIREMENTS. ADDITIONAL INFORMATION ON COMMAND AND SPECIFIC SYSTEMS STATUS IS AVAILABLE IN SEVERAL DITPR-DON FISMA METRICS. THESE REPORTS AND METRICS ALLOW NAVY COMMAND INFORMATION OFFICERS (IO), OPNAV N6, AND HQMC C4 TO EASILY ACCESS DATA TO MONITOR AND ADDRESS COMPLIANCE STATUS ISSUES BEFORE A SYSTEM REACHES A NON-COMPLIANT STATUS.

8. MAINTAINING SYSTEM ACCREDITATION AND TESTING SYSTEMS ANNUALLY FOR VARIOUS FISMA REQUIREMENTS, AS WELL AS ACCURATE DITPR-DON REPORTING, MUST BE A TOP INFORMATION ASSURANCE PRIORITY FOR EACH COMMAND IO, PROGRAM MANAGER, AND INFORMATION SECURITY OFFICIALS AT ALL NAVY AND MARINE CORPS COMMANDS, ESPECIALLY IN VIEW OF THE EVER-INCREASING THREAT TO DOD IT ASSETS.

9. REQUEST WIDEST DISSEMINATION OF THIS MESSAGE.

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