

DON CIO Message DTG: 081605Z JAN 09
SUBJ/DEPARTMENT OF THE NAVY FEDERAL INFORMATION SECURITY MANAGEMENT ACT
GOALS FOR FY 2009//

UNCLASSIFIED//
MSGID/GENADMIN/DON CIO WASHINGTON DC//

REF/A/DOC/FISMA/23JAN2002//
REF/B/DOC/DITPR-DON REGISTRATION GUIDANCE/JUNE 2006//
REF/C/DOC/DOD INFORMATION ASSURANCE CERTIFICATION AND ACCREDITATION
PROCESS/28NOV07//
REF/D/DOC/DON IT POLICY GUIDANCE FOR FY2009/20 AUG 2008//

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), 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 FY2009, 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:703-412-4681/EMAIL: JENNIFER.ELLETT.CTR@NAVY.MIL
POC/JAMES COLLINS/CTR/DON CIO/LOC: WASHINGTON DC/TEL:703-602-6202/
EMAIL: JAMES.E.COLLINS.CTR@NAVY.MIL//
POC/RAY LETTEER/CIV/HQMC C4/: WASHINGTON DC/TEL: 703-693-3490/EMAIL:
RAY.LETTEER@USMC.MIL//
POC/CHARLES BUCKLEY/CAPT/HQMC C4/LOC: WASHINGTON DC/TEL: 703-693-3490/
EMAIL: CHARLES.BUCKLEY@USMC.MIL//
POC/JOYCE DAWKINS/CIV/OPNAV N6132/LOC: WASHINGTON DC/TEL: (703) 601-
1710
/EMAIL: JOYCE.DAWKINS@NAVY.MIL //
POC/TONY PLATER/CTR/OPNAV N61/LOC: WASHINGTON DC/TEL:
703-601-1367/EMAIL: ALVIN.PLATER.CTR@NAVY.MIL//

RMKS/1. THIS MESSAGE PROVIDES DEPARTMENT OF THE NAVY (DON) FEDERAL
INFORMATION SECURITY MANAGEMENT ACT (FISMA) GOALS FOR FY09, INCLUDING
QUARTERLY REPORTING REQUIREMENTS.

2. BACKGROUND: FISMA (REF A) REQUIRES THAT EACH FEDERAL AGENCY REPORT
A SUMMARY STATUS OF INFORMATION TECHNOLOGY (IT) 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. IN FY09 IT IS CRITICAL THAT ALL
NAVY AND MARINE CORPS SYSTEMS OPERATE IN FULL COMPLIANCE WITH THE FISMA
REPORTING REQUIREMENTS. THE DON AND DEPARTMENT OF DEFENSE (DOD) MUST

REPORT TO OMB QUARTERLY WITH DETAILED STATISTICS ON COMPLIANCE WITH FISMA REQUIREMENTS. OMB, DOD, AND THE DON ARE CLOSELY MONITORING THESE STATISTICS TO ENSURE COMPLIANCE WITH REQUIREMENTS IS CONTINUALLY MAINTAINED.

3. ACTION FOR ALL DON:

A. IN ACCORDANCE WITH REF B, SINCE 2006 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 ACHIEVE/MAINTAIN A 100 PERCENT ACCREDITATION (I.E., AUTHORIZATION TO OPERATE (ATO) OR INTERIM AUTHORIZATION TO OPERATE (IATO)).

(1) AS A REMINDER, REF C LIMITS IATOS TO 180 DAYS AND LIMITS CONSECUTIVE IATOS TO NO MORE THAN 360 DAYS. IF AN IATO IS REQUIRED FOR MORE THAN 360 DAYS, ONLY THE DON CHIEF INFORMATION OFFICER (CIO) MAY AUTHORIZE THE CONTINUED OPERATION OF THE SYSTEM.

(2) 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 DAA.

C. ACHIEVE/MAINTAIN 100 PERCENT COMPLIANCE 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.

D. ENSURE MILESTONES LISTED IN A SYSTEM'S POA&M ARE ACHIEVABLE AND MET WITHIN THE TIMELINE CONTAINED IN THE POA&M. THE DESIGNATED ACCREDITING AUTHORITIES (DAA) 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.

E. ACHIEVE/MAINTAIN AT LEAST 96 PERCENT ANNUAL SECURITY AWARENESS TRAINING FOR ALL USERS AND ENSURE THAT AT LEAST 90 PERCENT OF EMPLOYEES WITH SIGNIFICANT SECURITY RESPONSIBILITIES RECEIVE SPECIALIZED TRAINING BY 31 AUGUST 2009. THESE REQUIREMENTS ARE REQUIRED BY OMB AND ARE DIFFERENT FROM THE DOD INFORMATION ASSURANCE (IA) WORKFORCE CERTIFICATION REQUIREMENTS STATED IN THE DOD WORKFORCE MANUAL.

4. CONSEQUENCES FOR NON-COMPLIANCE:

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

B. COMPLIANCE WILL BE ASSESSED QUARTERLY, BASED ONLY ON DITPR-DON REPORTED DATA ON OR ABOUT 12 FEB 09, 13 MAY 09, AND 13 AUG 09.

C. SYSTEMS FOUND TO BE NON-COMPLIANT IN DITPR-DON AT ANY TIME MAY BE REVIEWED FOR ADDITIONAL CONSEQUENCES IN ADDITION TO THE FUND 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.

5. 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 4B. THEREFORE, THE DATES CALCULATED FOR OPEN WEAKNESSES PAST THE MILESTONE DATE SHOULD BE BASED ON THE NEXT QUARTERLY REPORTING DATE. FOR EXAMPLE, FOR THE QUARTERLY REPORT ON 12 FEB 08, SYSTEMS THAT ARE 90 TO 120 DAYS OVERDUE WILL HAVE POA&M MILESTONE DATES THAT FALL BETWEEN 15 OCTOBER 2008 AND 14 NOVEMBER 2008. SYSTEMS WITH MILESTONES MORE THAN 120 DAYS OVERDUE WILL HAVE MILESTONES DATES BEFORE 15 OCTOBER 2008.

D. SYSTEMS MORE THAN 90 DAYS PAST A MILESTONE DATE WITH AN OPEN DEFICIENCY WILL ALSO HAVE TO 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 4B.

6. FOR INFORMATION, THE DON CIO WILL PROVIDE WEEKLY 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 ECHELON II COMMAND INFORMATION OFFICERS (IO), OPNAV N6, AND HQMC C4 TO EASILY ACCESS DATA TO MONITOR AND ADDRESS COMPLIANCE STATUS ISSUES BEFORE REACHING A NON-COMPLIANT STATUS.
7. MAINTAINING SYSTEM ACCREDITATION AND TESTING SYSTEMS ANNUALLY FOR VARIOUS FISMA REQUIREMENTS, AS WELL AS ACCURATE DITPR-DON REPORTING, MUST BE A TOP IA PRIORITY FOR EACH COMMAND IO, PROGRAM MANAGER, AND INFORMATION SECURITY OFFICIAL AT ALL NAVY ECHELON II COMMANDS AND MARINE CORPS MAJOR SUBORDINATE COMMANDS WITHIN THE DON, ESPECIALLY IN VIEW OF THE EVER-INCREASING THREAT TO DOD IT ASSETS AND THE GLOBAL WAR ON TERRORISM.
8. REQUEST WIDEST DISSEMINATION OF THIS MESSAGE.
9. RELEASED BY ROBERT J. CAREY, DEPARTMENT OF THE NAVY CHIEF INFORMATION OFFICER.//