MCBUL 5239. USMC INFORMATION ASSURANCE VULNERABILITY MANAGEMENT (IAVM) PROGRAM
Date Signed: 11/19/2008
MARADMIN Number: 639/08
R 131913Nov08Z
MARADMIN 639/08
MSGID/GENADMIN/CMC WASHINGTON DC C4 IA//
SUBJ/MCBUL 5239. USMC INFORMATION ASSURANCE
/VULNERABILITY MANAGEMENT (IAVM) PROGRAM//
REF/A/MSGID:GENADMIN/COMMARFOR CND/121830ZDEC2000/-/NOTAL//
REF/B/MSGID:MARADMIN/CMC/271527ZJUN2003/-/NOTAL//
REF/C/MSGID:GENADMIN/CMC/060930ZMAR1998/-/NOTAL//
REF/D/MSGID:MSG/MCNOSC/121308ZAUG2003/-/NOTAL/-//
REF/E/MSGID:MSG/MCNOSC/161737ZJAN2004/-/NOTAL/-//
REF/F/MSGID:MSG/MCNOSC/062241ZJAN2006/-/NOTAL/-//
REF/G/MSGID:MSG/MCNOSC/021015ZMAY2008/-/NOTAL//
REF/H/MSGID:DOC/JTF GNO/-//
REF/I/MSGID:DOC/CJCSM 6510.01/YMD:20070314/-/-/-//
REF/J/MSGID:DOC/CJCSI 6211.02B/YMD:20030721//
REF/K/MSGID:DOC/MCIAED 016/YMD:20080110/-/NOTAL//
REF/L/MSGID:DOC/MCIAED 014/YMD:20070716/-/NOTAL//
REF/M/MSGID:DOC/SECNAV M-5214.1M/-//
REF/M/MSGID:DOC/MCIAED 014/-//
NARR/REF A DEFINES THE CURRENT PROCESS SUPPORTING THE USMC IAVM PROGRAM. REF B IS MARADMIN 313/03, WHICH ANNOUNCED THE ESTABLISHMENT OF THE MARINE CORPS NETWORK OPERATIONS AND SECURITY CENTER (MCNOSC) AND DESCRIBED ITS ROLES AND RESPONSIBILITIES. REF C IS THE USMC NOC CONOPS, WHICH ESTABLISHED A FOUR-TIERED 'ECHELONS OF SUPPORT' STRUCTURE FOR COMPUTER TECH SUPPORT AND NETWORK MANAGEMENT IN THE MARINE CORPS. REF D IS MARINE CORPS ENTERPRISE NETWORK (MCEN) OPERATIONAL DIRECTIVE (OPDIR) 001-03, WHICH PROVIDED GUIDANCE FOR DELIVERY OF USMC-EDS INTEGRATED TECHNICAL SUPPORT DURING NMCI AOR. REF E IS OPDIR 007-04, WHICH PROVIDED GUIDANCE FOR THE DEVELOPMENT OF A MARINE CORPS IAVM PROGRAM. REF F IS OPDIR 006-06 THAT ESTABLISHES AND DIRECTS WEB-BASED OPDIR REPORTING VIA OPERATIONAL DIRECTIVE REPORTING SYSTEM (OPDRS). REF G ESTABLISHES THE C2 STRUCTURE FOR EXECUTING NETOPS WITHIN THE MARINE CORPS. REF H IS CTO 08-05, WHICH MANDATED THAT EACH SERVICE EMPLOYS AN IAVM PROGRAM. REF I IS THE DEFENSE IN DEPTH, COMPUTER NETWORK DEFENSE DIRECTIVE. REF J IS THE DEFENSE INFORMATION SYSTEMS NETWORK (DISN) POLICY, RESPONSIBILITIES AND PROCESSES. REF K IS THE MARINE CORPS INFORMATION ASSURANCE ENTERPRISE DIRECTIVE (MCIAED) 016, WHICH PROVIDES GUIDANCE ON THE CONDUCT OF VULNERABILITY ASSESSMENTS. REF L IS MCIAED 014, WIRELESS LOCAL AREA NETWORKS. REF M IS THE DON INFORMATION REQUIREMENTS (REPORTS) MANUAL.
REPORT REQUIRED: INFORMATION ASSURANCE VULNERABILITY MANAGEMENT DATA (REPORT CONTROL SYMBOL EXEMPT) PAR. 4.A.3, 4.A.8, 4.D.4, 4.E.2, 5.E.2. THESE REPORTING REQUIREMENTS ARE EXEMPT FROM REPORTS CONTROL ACCORDING TO REF L, PART IV, PARAGRAPH 7.J//
POC/RAY A. LETTEER/CIV/UNIT:HQMC C4 IAD/NAME: COMM 703-693-3490
/TEL:DSN 223-3490/EMAIL:RAY.LETTEER@USMC.MIL//
POC/GLEN FOSTER/CIV/UNIT:MCNOSC VMT/NAME: COMM 703-432-6747
/EMAIL:FOSTERGM@MCNOSC.USMC.MIL//
GENTEXT/REMARKS/1. PURPOSE. THIS IS A HEADQUARTERS, U.S. MARINE CORPS, COMMAND, CONTROL, COMMUNICATIONS AND COMPUTERS (C4) DEPT, MCNOSC COORDINATED MESSAGE, WHICH PROVIDES UPDATED GUIDANCE FOR THE EXECUTION OF THE MARINE CORPS IAVM PROGRAM.

DISTRIBUTION: PCN 10207718400
DISTRIBUTION STATEMENT A: APPROVED FOR PUBLIC RELEASE; DISTRIBUTION IS UNLIMITED.

2. CANCELLATION. THIS MESSAGE SUPERCEDES AND CANCELS REFS A, C, AND E.

3. BACKGROUND.

A. THE DEPARTMENT OF DEFENSE (DOD) IAVM PROGRAM IS DESIGNED TO PROVIDE POSITIVE CONTROL OF THE VULNERABILITY NOTIFICATION AND CORRECTIVE ACTION PROCESS WITHIN DOD INFORMATION SYSTEMS. THE JOINT TASK FORCE GLOBAL NETWORK OPERATIONS (JTF-GNO) MANAGES THE EXECUTION OF THE DOD IAVM PROGRAM.

B. PER REF B, THE MCNOSC IS THE SERVICE COMPONENT TO JTF-GNO AND IS THE USMC REPORTING AGENT FOR THE DOD IAVM PROGRAM. THE VULNERABILITY MANAGEMENT TEAM (VMT) IS THE PRIMARY AGENT WITHIN THE MCNOSC DESIGNATED TO MANAGE THE USMC VULNERABILITY MANAGEMENT PROGRAM IN SUPPORT OF THE JTF-GNO AND DOD IAVM PROGRAM.

C. THE MARINE CORPS IAVM PROGRAM RESPONSIBILITIES ARE ACCOMPLISHED USING THE NETOPS COMMAND AND CONTROL STRUCTURE IDENTIFIED IN REF G. THE FOLLOWING PROVIDES GUIDANCE FOR THE EXECUTION OF THE MARINE CORPS IAVM PROGRAM.

4. POLICY.

A. MCNOSC VULNERABILITY MANAGEMENT TEAM (VMT) WILL:

(1) MAINTAIN ACCESS AND ADMINISTRATION OF THE USMC VULNERABILITY MANAGEMENT SYSTEM (VMS) PRESENCE.

(2) ENSURE DISSEMINATION OR AVAILABILITY OF IAVM VULNERABILITY NOTIFICATIONS FOR PERSONNEL RESPONSIBLE FOR IMPLEMENTING AND MANAGING RESPONSES TO INFORMATION SYSTEMS VULNERABILITIES.

(3) ENTER MARINE CORPS ORGANIZATIONS COMPLIANCE DATA INTO THE VMS.

(4) MONITOR AND ENFORCE IAVA COMPLIANCE, SECURITY TECHNICAL IMPLEMENTATION GUIDE (STIG) COMPLIANCE, POA&MS, AND MITIGATION STATUS TO INCLUDE WIRELESS VULNERABILITY ASSESSMENTS PER REF K.

(5) ESTABLISH A PROCESS TO INFORM MCEN DESIGNATED APPROVING AUTHORITY (DAA) AND SENIOR LEADERSHIP OF NON COMPLIANT COMMANDS.

(6) MANAGE THE MARINE CORPS VULNERABILITY SCANNING PROCESS IDENTIFIED IN REF H.

(7) CONDUCT VULNERABILITY SCANS OF ALL MCEN ASSETS TO VALIDATE COMPLIANCE, ASSESS RISK, OR GAIN SITUATIONAL AWARENESS. VMT WILL COORDINATE SCANS IAW STANDARD MCNOSC PROCEDURES.

(8) MONITOR FINDINGS, ENFORCE REQUIRED MITIGATIONS, AND REPORT COMPLIANCE TO THE JTF-GNO ON ENHANCED COMPLIANCE VALIDATION VISITS CONDUCTED BY DEFENSE INFORMATION SYSTEM AGENCY (DISA).

B. PROGRAM MANAGERS (PMS).

(1) PUBLISH PROGRAM COMPLIANCE ACTIONS IN THE FORM OF A PROGRAM ACTION AND PLAN AND, IF APPLICABLE, A POA&M (INCLUDING MITIGATION ACTIONS) FOR EVERY DOD IAVM NOTIFICATION ISSUED.

(2) RESPOND TO EACH VULNERABILITY NOTIFICATION AS THE SYSTEM CONFIGURATION MANAGER.

(3) ESTABLISH A CAPABILITY TO IMPLEMENT CRITICAL PATCHES OR MITIGATIONS AS IDENTIFIED IN THE VULNERABILITY NOTICES WITHIN THE REQUIRED TIMELINES.

(4) PROVIDE COMPLIANCE ACTIONS AND IF APPLICABLE, (I.E., ASSETS CANNOT BE MADE COMPLIANT), A POA&M, INCLUDING MITIGATION ACTIONS, TO SYSTEM USERS.

(5) DIRECT COMPLIANCE ACTIONS AND POA&MS TO ADDRESS SPECIFIC ACTIONS TAKEN TO MITIGATE RISKS IDENTIFIED IN IAVAS.

(6) ENSURE DISSEMINATION OF COMPLIANCE ACTIONS AND, IF APPLICABLE, POA&MS TO AFFECTED SYSTEM ADMINISTRATORS.

(7) ESTABLISH A DOCUMENTED PROCESS TO TEST PATCHES BEFORE THEY ARE APPLIED TO CRITICAL SYSTEMS.

(8) ENSURE ALL ASSETS HAVE UP TO DATE ANTIVIRUS ENGINE AND SIGNATURES.

(9) ENSURE HOST BASED SECURITY SYSTEM (HBSS) AGENTS AND BELMANAGE AGENTS ARE INSTALLED ON ALL APPLICABLE ASSETS.

C. COMMAND/LOCAL INFORMATION ASSURANCE MANAGERS (IAMS).

(1) ADVISE AND ASSIST THE MCEN DAA ON THE VULNERABILITY MANAGEMENT (VM) PROGRAM.

(2) MONITOR VM NOTIFICATION MESSAGES AND REPORT COMPLIANCE TO MCNOSC VMT.

(3) ENSURE DEVELOPMENT OF POA&MS, MITIGATION ACTIONS, AND COMPLIANCE TIMELINES AS REQUIRED.

(4) COMPLY WITH ALL VULNERABILITY RELATED OPERATIONAL DIRECTIVES WITHIN THE REQUIRED DEADLINES.

(5) CONDUCT MONTHLY VULNERABILITY SCANS IAW REF H. IMMEDIATELY UPON COMPLETION OF SCANS REMEDIATE ALL OPEN VULNERABILITIES AND CORRECT CONFIGURATION ISSUES.

(6) MAINTAIN STIG COMPLIANCE ON ALL MCEN ASSETS.

(7) ALLOW THE VMT ACCOUNTS AND APPROPRIATE PERMISSIONS AND REGISTRY ACCESS TO ALL ASSETS FOR THE PURPOSE OF SCANNING. THIS INCLUDES ADMINISTRATIVE ACCESS TO RETINA AND HERCULES SERVERS.

(8) ESTABLISH A DOCUMENTED PROCESS TO TEST PATCHES BEFORE THEY ARE APPLIED TO CRITICAL SYSTEMS.

(9) USE THE DOD AND USMC APPROVED VULNERABILITY SCANNING AND REMEDIATION TOOLS. WHEN THESE TOOLS DO NOT SUPPORT THE TECHNOLOGIES USED I.E., IF HERCULES DOES NOT SUPPORT A REQUIRED REMEDIATION OR RETINA CANNOT SCAN A PARTICULAR OS/APPLICATION, HAVE THE CAPABILITY TO MANUALLY IDENTIFY AND REMEDIATE VULNERABLE SYSTEM OR HAVE ANOTHER DEPARTMENT OF THE NAVY, APPLICATION AND DATABASE MANAGEMENT SYSTEM (DADMS)APPROVED TOOL WITH WHICH TO SCAN OR REMEDIATE.

(10) ENSURE ALL ASSETS HAVE UPDATED ANTIVIRUS ENGINE AND SIGNATURES.

(11) ENSURE HBSS AGENTS AND BELMANAGE AGENTS ARE INSTALLED ON ALL APPLICABLE ASSETS

D. SYSTEMS ADMINISTRATORS/GREEN/BLUE TEAM MEMBERS.

(1) ENSURE ALL ASSETS ARE COMPLIANT WITH APPLICABLE MCEN POLICY AND OPERATIONAL DIRECTIVES.

(2) CONDUCT PERIODIC VULNERABILITY ASSESSMENTS PER REF F. ASSETS FOUND NON-COMPLIANT MUST BE HANDLED PER REF I.

(3) CONDUCT QUARTERLY WAR-DRIVING WIRELESS DETECTION ASSESSMENTS AND REPORT ROGUE DEVICES TO MCNOSC VMT.

(4) REPORT NON COMPLIANT PM MANAGED PROGRAMS THAT HAVE NOT COMPLIED WITH DIRECTED VULNERABILITY MANAGEMENT GUIDANCE.

(5) REF I, PAR. 5K3 DIRECTS SYSTEMS ADMINISTRATORS TO MONITOR APPROPRIATE WEB SITES FOR NEW VULNERABILITIES AND APPLY ALL RELEVANT SECURITY PATCHES. NOTE: USMC IAMS AND ADMINISTRATORS MUST TAKE A PROACTIVE APPROACH TO APPLYING ALL SECURITY PATCHES TO SYSTEMS ON THE MCEN. IAVM AND OPDIR NOTICES ARE MEANT TO PRIORITIZE PATCHING EFFORTS AND ONLY IDENTIFY THE MOST CRITICAL PATCHES THAT MUST BE APPLIED IMMEDIATELY TO MITIGATE SIGNIFICANT THREATS. ADMINISTRATORS, IAMS, AND IA LEADERS WILL PRACTICE AND ENCOURAGE PROACTIVE PATCHING OF ALL SECURITY THREATS, TO INCLUDE IAVM AND OPDIR DIRECTED PATCHES.

(6) TEST ALL PATCHES, CONFIGURATION CHANGES, AND UPGRADES PRIOR TO INSTALLATION ON PRODUCTION NETWORKS.

(7) CONDUCT MONTHLY VULNERABILITY SCANS OF ALL COMMAND ASSETS PER REF H.

(8) USE THE DOD AND USMC APPROVED VULNERABILITY SCANNING AND REMEDIATION TOOLS. WHEN THESE TOOLS DO NOT SUPPORT THE TECHNOLOGIES USED. (I.E., IF HERCULES DOES NOT SUPPORT A REQUIRED REMEDIATION OR RETINA CANNOT SCAN A PARTICULAR OS/APPLICATION), HAVE THE CAPABILITY TO MANUALLY IDENTIFY AND REMEDIATE VULNERABLE SYSTEMS OR HAVE ANOTHER DEPT OF NAVY APPLICATION DATABASE MANAGEMENT SYSTEM (DADMS) APPROVED TOOLS WITH WHICH TO SCAN OR REMEDIATE.

(9) ENSURE ALL ASSETS HAVE UPDATED ANTIVIRUS ENGINE AND SIGNATURES.

(10) ENSURE HBSS AGENTS AND BELMANAGE AGENTS ARE INSTALLED ON ALL APPLICABLE ASSETS

E. NMCI VENDOR (EDS):

(1) ENSURE ALL ASSETS ARE OPERATIONAL DIRECTIVE COMPLIANT.

(2) MONITOR VM NOTIFICATION MESSAGES AND REPORT COMPLIANCE TO MCNOSC VMT.

(3) ENSURE DEVELOPMENT OF POA&MS, MITIGATION ACTIONS, AND COMPLIANCE TIMELINES AS REQUIRED.

(4) COMPLY WITH ALL VULNERABILITY RELATED OPERATIONAL DIRECTIVES WITHIN THE REQUIRED DEADLINES.

(5) CONDUCT MONTHLY VULNERABILITY SCANS IAW REF H. IMMEDIATELY UPON COMPLETION OF SCANS REMEDIATE ALL OPEN VULNERABILITIES AND CORRECT CONFIGURATION ISSUES.

(6) MAINTAIN STIG COMPLIANCE ON ALL MCEN ASSETS.

(7) ALLOW THE VMT ACCESS AND APPROPRIATE PERMISSIONS AND REGISTRY ACCESS TO ALL NON-NMCI ASSETS FOR THE PURPOSE OF SCANNING. THIS INCLUDES ADMINISTRATIVE ACCESS TO RETINA AND HERCULES SERVERS.

(8) ESTABLISH A DOCUMENTED PROCESS TO TEST PATCHES BEFORE THEY ARE APPLIED TO CRITICAL SYSTEMS.

(9) USE THE DOD AND USMC APPROVED VULNERABILITY SCANNING AND REMEDIATION TOOLS. WHEN THESE TOOLS DO NOT SUPPORT THE TECHNOLOGIES USED (I.E., IF HERCULES DOES NOT SUPPORT A REQUIRED REMEDIATION OR RETINA CANNOT SCAN A PARTICULAR OS/APPLICATION) HAVE THE CAPABILITY TO MANUALLY IDENTIFY AND REMEDIATE VULNERABLE SYSTEMS OR HAVE ANOTHER DADMS APPROVED TOOLS WITH WHICH TO SCAN OR REMEDIATE.

(10) PRACTICE AND ENCOURAGE PROACTIVE PATCHING OF ALL SECURITY THREATS NOT JUST IAVM AND OPDIR DIRECTED PATCHES.

F. DEFINITIONS.

(1) CENTRALLY MANAGED SYSTEM. USE OF THE PHRASE 'CENTRALLY MANAGED SYSTEM' IN THIS MESSAGE REFERS TO A SYSTEM FOR WHICH CONFIGURATION CONTROL IS EXERCISED BY A CENTRAL AUTHORITY (E.G., PROGRAM OFFICE). CENTRALLY MANAGED SYSTEMS MAY BE MARINE CORPS 'OWNED' (E.G., IAS) OR THEY MAY BE CONTROLLED BY OTHER DOD SERVICES AND AGENCIES EXTERNAL TO THE MARINE CORPS (E.G., GLOBAL COMMAND AND CONTROL SYSTEM (GCCS), UNIT DIARY MARINE INTEGRATED PERSONNEL SYSTEM (UDMIPS), ETC.). 'MARINE CORPS' OWNED SYSTEMS ALSO INCLUDE SOFTWARE PRODUCED BY THE MARINE CORPS, WHICH IS USED BY OTHER DOD SERVICES AND AGENCIES. CENTRALLY MANAGED SYSTEMS ARE SUBJECT TO THE IAVM PROGRAM. HOWEVER, ORGANIZATIONS (E.G., MARINE CORPS UNITS OR NMCI VENDOR) HOSTING AND OPERATING A CENTRALLY MANAGED SYSTEM MUST OBTAIN APPROVAL FROM ITS CONFIGURATION CONTROL AUTHORITY BEFORE IMPLEMENTING IAVM PROGRAM DIRECTED ACTIONS.

(2) LOCALLY MANAGED SYSTEM. USE OF THE PHRASE 'LOCALLY MANAGED SYSTEM' IN THIS MESSAGE REFERS TO SYSTEMS (LEGACY OR OTHERWISE) WHERE CONFIGURATION CONTROL IS EXERCISED BY THE LOCAL ORGANIZATION THAT IS OPERATING THE SYSTEM. NO OUTSIDE APPROVAL IS REQUIRED PRIOR TO IMPLEMENTING IAVM PROGRAM DIRECTED ACTIONS ON A LOCALLY MANAGED SYSTEM.

(3) SYSTEM ADMINISTRATION (SYSADMIN). USE OF THE TERM 'SYSADMIN' IN THIS MESSAGE REFERS TO ACCESS AND AUTHORITY TO CONTROL THE DAILY OPERATION AND MAINTENANCE OF A SYSTEM. IMPLEMENTATION OF IAVM DIRECTED ACTIONS ARE ACCOMPLISHED THROUGH THE SYSADMIN. THE DISTINCTION BETWEEN 'CONFIGURATION CONTROL' AND 'SYSADMIN' IS THAT SYSTEM CHANGES ARE 'AUTHORIZED' BY THE CONFIGURATION CONTROL AUTHORITY AND 'IMPLEMENTED' BY SYSADMIN.

(4) MARINE CORPS ENTERPRISE NETWORK (MCEN). THE MCEN REPRESENTS THE TOTALITY OF THE MARINE CORPS' GENERAL SERVICE NETWORK ENVIRONMENT. THE MCEN IS COMPRISED OF SUPPORTING ESTABLISHMENT NETWORKS; NMCI, LEGACY AND DEPLOYED/TACTICAL (BOTH NIPRNET AND SIPRNET), AND INFRASTRUCTURE THAT PROVIDES ACCESS TO DISA MANAGED MAINFRAME COMPUTER SERVICES. THE MCEN CONSISTS OF TWO MAJOR SUBDIVISIONS, WHICH ARE DISTINGUISHED BY THEIR RELATIONSHIP TO NMCI.

(A) USMC NMCI COI. SYSTEMS WITHIN NMCI SUPPORTING THE MARINE CORPS WILL BE MANAGED AS A SEPARATE COMMUNITY OF INTEREST

(USMC NMCI COI). THE USMC NMCI COI IS A SUBSET OF THE MCEN AND IT INCLUDES:

1. ASSETS IN NMCI ASSUMPTION OF RESPONSIBILITY (AOR) STATUS. NMCI TRANSITION BEGINS WITH AOR OF THE 'AS IS' LEGACY NETWORK INFRASTRUCTURE BY THE VENDOR. ASSETS ENTER AOR STATUS WHEN SYSADMIN TRANSFERS FROM THE GOVERNMENT TO EDS.

2. ASSETS IN NMCI CUTOVER/TRANSITIONED STATUS. CUTOVER IS ACHIEVED WHEN A SERVICE OR SYSTEM IS FULLY TRANSITIONED FROM THE AOR ENVIRONMENT INTO THE NMCI NETWORK. THE VENDOR PERFORMS SYSADMIN ON ALL CUTOVER AND FULLY TRANSITIONED NMCI ASSETS.

3. MARINE CORPS MANAGED ASSETS IN NMCI. DURING AOR, CUTOVER AND POST-NMCI TRANSITION, THE MARINE CORPS WILL RETAIN SYSADMIN CONTROL OVER A NUMBER OF SYSTEMS (E.G., LEGACY APPLICATION SERVERS) OPERATING WITHIN NMCI.

(B) NON-NMCI MCEN. NON-NMCI MCEN REFERS TO THAT PORTION OF THE MCEN WHICH IS NOT PART OF NMCI. THIS INCLUDES ASSETS THAT ARE NOT PLANNED TO BECOME PART OF NMCI. NOTE THAT 'NON-NMCI MCEN' STATUS APPLIES TO NMCI ASSETS THAT ARE REMOVED FROM NMCI AND USED BY MARINE CORPS UNITS IN A DEPLOYED ENVIRONMENT (E.G., AFLOAT AND TACTICAL NETWORKS). MARINE CORPS UNITS WILL EXERCISE SYSADMIN CONTROL OVER THESE ASSETS WHILE THEY ARE DEPLOYED OUTSIDE OF NMCI. UPON RETURN FROM DEPLOYMENT, THESE SYSTEMS WILL BE RE-INTRODUCED INTO THE USMC NMCI COI AND SYSADMIN WILL BE RETURNED TO EDS CONTROL.

5. PROCESS. USMC VM PROCESS. THE USMC VM PROGRAM ENCOMPASSES BOTH THE SENSITIVE BUT UNCLASSIFIED (NIPRNET) AND THE CLASSIFIED (SIPRNET) PORTIONS OF THE MCEN. IT APPLIES TO USMC NMCI COI AND TO NON-NMCI MCEN ASSETS AND TO BOTH CENTRALLY AND LOCALLY MANAGED SYSTEMS. THE USMC VM PROCESS CONTAINS THE FOLLOWING STEPS:

A. JTF-GNO ASSESSES ALL VULNERABILITIES RELEASED ON THE INTERNET AND DETERMINES THE THREAT TO THE DOD ENTERPRISE. WHEN SIGNIFICANT THREATS WARRANT ACTION, THE JTF-GNO PROMULGATES THIS INFORMATION VIA FORMAL MESSAGE TRAFFIC. THERE ARE THREE TYPES OF IAVM MESSAGES RELEASED BY THE JTF-GNO. THESE ARE:

(1) INFORMATION ASSURANCE VULNERABILITY ALERT (IAVA). IAVA MESSAGES ARE GENERATED WHEN A NEW VULNERABILITY TO A SYSTEM EXISTS THAT POSES AN IMMEDIATE AND SIGNIFICANT THREAT TO THE DOD. JTF-GNO REQUIRES ACKNOWLEDGEMENT OF RECEIPT AND COMPLIANCE REPORTING ON IAVA MESSAGES. IAVA'S DO NOT EXPIRE UNTIL DIRECTED BY THE JTF-GNO. COMPLIANCE MUST BE CONTINUOUSLY MAINTAINED ON ALL AFFECTED SYSTEMS UNTIL THEY ARE REMOVED FROM SERVICE OR REPLACED/UPGRADED BY A SYSTEM THAT DOES NOT HAVE THE ASSOCIATED VULNERABILITY.

(2) INFORMATION ASSURANCE VULNERABILITY BULLETIN (IAVB). IAVB MESSAGES ADDRESS NEW VULNERABILITIES THAT DO NOT POSE AN IMMEDIATE THREAT TO THE DOD, BUT A POTENTIAL FOR ESCALATION EXISTS IF CORRECTIVE ACTION IS NOT TAKEN. THEREFORE, COMPLIANCE IS MANDATORY. JTF-GNO REQUIRES ACKNOWLEDGEMENT OF RECEIPT ONLY FOR IAVB MESSAGES.

(3) TECHNICAL ADVISORY (TA). TECHNICAL ADVISORIES ADDRESS LOW RISK VULNERABILITIES AND ARE PROVIDED FOR INFORMATIONAL PURPOSES.

B. MCNOSC VMT:

(1) THE VMT WILL ACKNOWLEDGE RECEIPT OF IAVA AND IAVB MESSAGES WITHIN THE DEADLINE REQUIRED BY JTF-GNO. TA MESSAGES DO NOT REQUIRE ACKNOWLEDGEMENT OF RECEIPT.

(2) THE VMT WILL CONDUCT AN INITIAL TECHNICAL ASSESSMENT OF THE IAVM MESSAGE TO DETERMINE ITS APPLICABILITY TO MARINE CORPS NETWORKS. THE MCNOSC VMT WILL DIRECT TASKS VIA OPERATIONAL DIRECTIVES (OPDIR). THESE DIRECTIVES WILL BE SENT TO MARFORS AND MAJOR SUPPORTING ESTABLISHMENT (SE) COMMANDS IDENTIFIED IN REF G. THESE IAVM RELATED OPERATIONAL DIRECTIVES WILL BE TAILORED TO THE SPECIFIC INFORMATION TECHNOLOGY ENVIRONMENT OF THE MARINE CORPS WITH MANDATED COMPLIANCE AND REPORTING REQUIREMENTS. PER REF D, ALL IAVA'S, IAVB'S, AND TA'S, WILL BE DISSEMINATED BY THE MCNOSC AS MCEN OPERATIONAL DIRECTIVE (OPDIR) MESSAGES. OPDIR MESSAGES WILL BE DISSEMINATED

THROUGHOUT THE MARINE CORPS, VIA AUTOMATIC MESSAGE HANDLING SYSTEM (AMHS), FOR APPROPRIATE ACTION. THE MCNOSC SHALL ALSO PROVIDE COPIES OF THESE MESSAGES, VIA EMAIL ATTACHMENT, TO EDS AT THE SAME TIME OF RELEASE TO THE MARINE CORPS. THE MCNOSC SHALL MAINTAIN ELECTRONIC COPIES OF ALL MARINE CORPS VULNERABILITY RELATED PROGRAM MESSAGES ON ITS WEB SITE AT URL WWW.MCNOSC.USMC.SMIL.MIL.

(3)IN ADDITION TO IAVM NOTICES RELEASED BY THE JTF-GNO, REF I REQUIRES THE USMC TO EVALUATE ALL OTHER SOFTWARE VULNERABILITIES AND DETERMINE THE RISK THEY POSE TO THE MCEN. WHEN THE RISK IS SIGNIFICANT VMT IS REQUIRED TO IDENTIFY MITIGATIONS, DIRECT COMPLIANCE, AND ESTABLISH REPORTING TIMELINES. GUIDANCE WILL BE ISSUED IN THE FORM OF AN OPERATIONAL DIRECTIVE. COMMANDS ARE REQUIRED TO COMPLY WITH THE REQUIRED ACTIONS WITHIN THE DEADLINES OUTLINED IN THE DIRECTIVE.

C. CONFIGURATION CONTROL AUTHORITIES (E.G., PROGRAM OFFICES).

(1) ISSUE APPROVAL TO APPLY MCNOSC DIRECTED CORRECTIVE ACTIONS TO CENTRALLY MANAGED SYSTEMS. ORGANIZATIONS (E.G., LOCAL MARINE CORPS COMMANDS OR NMCI VENDOR) MAY NOT APPLY CORRECTIVE MEASURES TO A CENTRALLY MANAGED SYSTEM UNTIL APPROVAL IS RECEIVED FROM THE CONFIGURATION CONTROL AUTHORITY. IN CASES WHERE MULTIPLE SYSTEMS ARE HOSTED ON A SINGLE PLATFORM, APPROVAL MUST BE OBTAINED FROM EACH RESPECTIVE CONFIGURATION CONTROL AUTHORITY BEFORE VULNERABILITY MITIGATION ACTIONS MAY BE IMPLEMENTED ON THE DEVICE. THIS IS DONE TO ENSURE OPERATIONAL FUNCTIONALITY, SECURITY, AND CONFIGURATION MANAGEMENT CONTROL.

(2) FOR IAVM RELATED OPERATIONAL DIRECTIVES WITH MANDATORY COMPLIANCE AND REPORTING REQUIREMENTS, THE FOLLOWING DIRECTION IS GIVEN TO MARINE CORPS COMMANDS THAT EXERCISE CONFIGURATION CONTROL AUTHORITY OVER A CENTRALLY MANAGED SYSTEM:

(A) MARINE CORPS SYSTEMS. ORGANIZATIONS THAT CENTRALLY MANAGE MARINE CORPS SYSTEMS ARE DIRECTED TO ASSESS THE IMPACT OF IMPLEMENTING THE PRESCRIBED CORRECTIVE ACTIONS FOR EACH IAVM RELATED OPERATIONAL DIRECTIVE MESSAGE WITH MANDATED COMPLIANCE REQUIREMENTS. THIS SHALL BE ACCOMPLISHED BY THE DEADLINE SPECIFIED IN THE DIRECTIVE MESSAGE. BY THE SPECIFIED DEADLINE, EACH CONFIGURATION CONTROL AUTHORITY MUST EITHER PROVIDE ORGANIZATIONS THAT HOST AND OPERATE (I.E., SYSADMIN) THE CENTRALLY MANAGED SYSTEM WITH PERMISSION TO APPLY CORRECTIVE ACTIONS, NOTIFY THEM THAT THE DIRECTIVE DOES NOT PERTAIN TO THE SYSTEM, OR THEY MUST NOTIFY THE MCNOSC OF ANY PROBLEMS THAT DO NOT PERMIT COMPLIANCE. THE MCNOSC MAY BE CONTACTED USING THE INFORMATION PROVIDED IN PARA 6 BELOW. IF A PROBLEM IS ENCOUNTERED WITH IMPLEMENTATION ON A CENTRALLY MANAGED SYSTEM, THE MCNOSC WILL WORK WITH THE JTF-GNO, MARCORSYSCOM, MCEN DAA, AND THE CONFIGURATION CONTROL AUTHORITY TO RESOLVE THE ISSUE.

(B) EXTERNALLY OWNED SYSTEMS. THE MARINE CORPS OPERATES SYSTEMS THAT ARE CENTRALLY MANAGED BY EXTERNAL ENTITIES (I.E., THOSE OWNED BY OTHER DOD SERVICES AND AGENCIES). ORGANIZATIONS RESPONSIBLE FOR OPERATING THESE EXTERNALLY MANAGED SYSTEMS SHALL:

1. ON BEHALF OF THE MARINE CORPS, TAKE ALL APPROPRIATE ACTION TO FACILITATE TIMELY APPROVAL FROM THE EXTERNAL CONFIGURATION CONTROL AUTHORITY TO APPLY IAVM CORRECTIVE MEASURES.

2. KEEP THE MCNOSC VMT AND THE ORGANIZATIONS (I.E., MARINE CORPS COMMANDS AND THE NMCI VENDOR) OPERATING THESE SYSTEMS (I.E., SYSADMIN) INFORMED OF PROGRESS BEING MADE TOWARD OBTAINING APPROVAL TO IMPLEMENT THE IAVM CORRECTIVE ACTIONS.

3. ALERT THE MCNOSC VMT WHEN APPROVAL IS NOT RECEIVED FROM THE EXTERNAL CONFIGURATION CONTROL AUTHORITY BY THE DEADLINE SPECIFIED IN THE DIRECTIVE. THIS WILL BE DONE BY NOTIFYING THE MCNOSC VMT USING THE CONTACT INFORMATION PROVIDED IN PARA 7 BELOW. THE MCNOSC WILL WORK WITH THE JTF-GNO, MCSC, MCEN DAA, THE RESPECTIVE MARINE CORPS PROGRAM OFFICE, AND THE EXTERNAL CONFIGURATION CONTROL AUTHORITY TO ADDRESS THE ISSUE.

D. IMPLEMENTATION OF VULNERABILITY RELATED CORRECTIVE ACTIONS. ALL MARINE CORPS ORGANIZATIONS AND THE NMCI VENDOR SHALL TAKE APPROPRIATE ACTION ON ALL VULNERABILITY RELATED OPERATIONAL DIRECTIVES. OPERATIONAL DIRECTIVES WITH MANDATED COMPLIANCE WILL REQUIRE MARINE CORPS ORGANIZATIONS AND THE NMCI VENDOR TO WORK AGGRESSIVELY IN ORDER TO ACHIEVE TIMELY COMPLIANCE AND ACCURATE REPORTING. APPROVAL TO APPLY DIRECTED ACTIONS ON CENTRALLY MANAGED SYSTEMS SUCH AS DMS, UDMIPS, NALCOMIS, AND GCCS SHALL BE RELEASED EXCLUSIVELY THROUGH THE RESPECTIVE CONFIGURATION CONTROL AUTHORITY (E.G., PROGRAM OFFICE). UNTIL THIS APPROVAL IS GIVEN, HOSTING ORGANIZATIONS WILL REPORT ON THESE SYSTEMS, BUT WILL NOT BE RESPONSIBLE FOR THEIR NON-COMPLIANT STATUS. HOWEVER, ONCE APPROVAL IS OBTAINED FROM THE PROGRAM OFFICE, ORGANIZATIONS OPERATING THOSE CENTRALLY MANAGED SYSTEMS WILL BE HELD ACCOUNTABLE FOR ACHIEVING FULL COMPLIANCE. EACH VULNERABILITY RELATED OPERATIONAL DIRECTIVE MESSAGE WITH MANDATED COMPLIANCE REQUIREMENTS WILL STATE THE DATE BY WHICH PROGRAM OFFICES MUST GIVE APPROVAL TO APPLY THE SPECIFIED CORRECTIVE ACTIONS. IF APPROVAL IS NOT RECEIVED BY THE SPECIFIED DATE IN THE MESSAGE, ORGANIZATIONS OPERATING THE SYSTEM SHALL NOTIFY THEIR RESPECTIVE THIRD ECHELON MCEN ORGANIZATION, WHO IN TURN WILL REPORT THIS INFORMATION TO THE MCNOSC VMT AND VIA OPDRS. THIS REPORT SHALL INCLUDE:

(1) NAME OF THE NONCOMPLIANT SYSTEM AND POINT OF CONTACT INFORMATION FOR THE SYSTEM CONFIGURATION CONTROL AUTHORITY (I.E., ORGANIZATION, NAME, TELEPHONE NUMBER, AND EMAIL ADDRESS).

(2) NAME OF THE UNIT(S) OPERATING THE SYSTEM AND POINT OF CONTACT INFORMATION (I.E., NAME, TELEPHONE NUMBER, AND EMAIL ADDRESS).

(3) NUMBER OF ASSETS AFFECTED (I.E., THE NUMBER OF SYSTEMS THAT ARE NON-COMPLIANT PENDING PROGRAM OFFICE APPROVAL TO APPLY THE IAVM ACTIONS).

(4) LAST KNOWN STATUS THAT WAS PROVIDED BY THE SYSTEM CONFIGURATION CONTROL AUTHORITY.

E. ORGANIZATIONS REPORT IAVM RELATED OPERATIONAL DIRECTIVE COMPLIANCE STATUS INFORMATION OR SUBMIT POA&M REQUESTS.

(1) COMPLIANCE REPORTING. FOR USMC OPERATIONAL DIRECTIVE MESSAGES THAT MANDATE COMPLIANCE AND REPORTING BY A SPECIFIED DEADLINE, THE FOLLOWING ADDITIONAL GUIDANCE IS PROVIDED:

(A) USMC NMCI COI. ASSETS IN THE USMC NMCI COI SHALL BE REPORTED AS FOLLOWS:

1. NMCI AOR. ASSETS IN NMCI AOR STATUS SHALL BE REPORTED BY THE GOVERNMENT, WITH INFORMATION AND ASSISTANCE PROVIDED BY LOCAL SITE NMCI VENDOR (EDS) PERSONNEL. EDS SHALL ACHIEVE COMPLETE AND TIMELY COMPLIANCE ON ALL ASSETS IN NMCI AOR STATUS AND PROVIDE REPORTING DATA TO THE SUPPORTED LOCAL MARINE CORPS ORGANIZATION. PER REF C, ALL THIRD ECHELON MCEN ORGANIZATIONS SHALL AGGREGATE REPORTING DATA FROM WITHIN THEIR RESPECTIVE AREA OF RESPONSIBILITY FOR SUBSEQUENT SUBMISSION TO THE MCNOSC. THEREFORE, PER REF E, MARINE CORPS ORGANIZATIONS AND LOCAL NMCI VENDOR PERSONNEL MUST WORK CLOSELY TOGETHER IN AN INTEGRATED AND MUTUALLY SUPPORTING EFFORT TO ACHIEVE AND REPORT COMPLIANCE FOR NMCI AOR ASSETS.

2. NMCI CUTOVER/TRANSITIONED ASSETS. EDS SHALL REPORT ON ALL ASSETS IN NMCI CUTOVER/TRANSITIONED STATUS THROUGH ITS INTERNAL CHAIN TO THE MCNOSC. THIS INFORMATION SHALL NOT BE INCLUDED IN GOVERNMENT COMPLIANCE REPORTS SUBMITTED TO THE MCNOSC BY MARINE CORPS ORGANIZATIONS.

3. MARINE CORPS MANAGED ASSETS. REPORTING OF ASSETS WITHIN THE NMCI NETWORK UNDER MARINE CORPS SYSADMIN CONTROL SHALL CONTINUE TO BE A GOVERNMENT RESPONSIBILITY. PER REF G, THE SIXTEEN TOP LEVEL COMMANDS IN THE USMC NETOPS C2 STRUCTURE SHALL AGGREGATE RESPONSES FROM SUBORDINATE ORGANIZATIONS FOR FURTHER SUBMISSION TO THE MCNOSC. THIS INFORMATION SHALL NOT BE INCLUDED IN NMCI VENDOR COMPLIANCE

REPORTS SUBMITTED TO THE MCNOSC BY EDS.

(2) NON-NMCI MCEN. REPORTING OF NON-NMCI MCEN ASSETS SHALL CONTINUE TO BE A GOVERNMENT RESPONSIBILITY. PER REF G, THE SIXTEEN TOP LEVEL COMMANDS IN THE USMC NETOPS C2 STRUCTURE SHALL AGGREGATE RESPONSES FROM SUBORDINATE ORGANIZATIONS FOR SUBSEQUENT SUBMISSION TO THE MCNOSC.

(3) DEPLOYED UNITS. FOR OFFICIAL IAVM RELATED OPERATIONAL DIRECTIVE REPORTING, DEPLOYED UNITS SHALL SUBMIT COMPLIANCE REPORTS TO THE SAME ENTITY AS WHEN IN GARRISON. HOWEVER, ADDITIONAL (E.G., DUAL) REPORTING MAY BE REQUIRED BY OPERATIONAL COMMANDERS.

(A) COMPLIANCE REPORT CONTENT. COMPLIANCE REPORTS MUST INCLUDE THE NUMBER OF ASSETS AFFECTED, THE NUMBER COMPLIANT, AND THE NUMBER OF UNPATCHED ASSETS FOR BOTH SIPRNET AND NIPRNET (BROKEN OUT SEPARATELY). ADDITIONALLY, COMMANDS MUST INDICATE THE CATEGORIES OF 'NON-NMCI' (DEFINED IN PARA 3D (2) ABOVE), 'NMCI AOR' (DEFINED IN PARA 3D (1) (A) ABOVE), OR 'IN NMCI AND UNDER MARINE CORPS SYSADMIN CONTROL' (DEFINED IN PARA 3D (1) (C) ABOVE). NEGATIVE RESPONSES ARE REQUIRED.

(B) METHOD OF COMPLIANCE REPORT SUBMISSION. IAVM COMPLIANCE REPORTS SHALL BE SUBMITTED IN ACCORDANCE WITH REF F.

(C) EXTENSION REQUESTS. EXTENSIONS ARE NOT AUTHORIZED IN THE DOD VULNERABILITY MANAGEMENT PROGRAM. IT IS RECOGNIZED THAT OPERATIONAL REQUIREMENTS MAY OCCASIONALLY PREVENT COMMANDS FROM ACHIEVING COMPLIANCE WITHIN PRESCRIBED DEADLINES. THE POA&M PROCESS OUTLINED IN REF I IS MEANT TO ACCOUNT FOR ASSETS THAT CANNOT BE PATCHED ON TIME. THE INTENT OF THE POA&M PROCESS IS TO DEVELOP A PLAN THAT ULTIMATELY ENDS WHEN ASSETS ARE PATCHED. THE POA&M ALSO REQUIRES COMMANDS TO IDENTIFY TEMPORARY MITIGATIONS THAT WILL PROTECT VULNERABLE ASSETS UNTIL THEY CAN BE PATCHED. THE JTF-GNO HAS FINAL REVIEW AUTHORITY OVER ALL MCEN POA&MS. DEPENDING ON THE LEVEL OF RISK INVOLVED, THE MCEN DAA MAY NOT APPROVE POA&M REQUESTS THAT INTRODUCE UNDUE RISK TO THE MCEN. AS SUCH, TIMELY AND AGGRESSIVE ACTION TO ACHIEVE AND MAINTAIN COMPLIANCE IS OF PARAMOUNT IMPORTANCE. HOWEVER, WHEN REQUIRED, REQUESTS FOR POA&MS SHALL BE SUBMITTED TO THE MCEN DAA VIA THE MCNOSC VMT. REQUESTS SHALL BE SUBMITTED TO THE MCNOSC VMT AS SOON AS THE NEED IS IDENTIFIED, BUT NOT LATER THAN THE POA&M DATE IDENTIFIED IN EACH OPERATIONAL DIRECTIVE. THE POA&M PROCESS IDENTIFIED IN THIS DOCUMENT WILL BE USED IN SUPPORT OF THE ECV PROCESS. ADDITIONAL GUIDANCE REGARDING POA&M REQUESTS IS AS FOLLOWS:

(D) RESPONSIBILITY FOR POA&M REQUEST SUBMISSION.

1. NMCI VENDOR (EDS). EDS SHALL SUBMIT POA&M REQUESTS ON VENDOR CONTROLLED ASSETS IN NMCI CUTOVER/TRANSITIONED STATUS DIRECTLY TO THE MCNOSC. WHENEVER THIS OCCURS, AFFECTED CERTIFYING AUTHORIZATION REPRESENTATIVES (CARS) AND INFORMATION ASSURANCE MANGERS (IAM'S) WILL BE INFORMED BY THE VENDOR. POA&M REQUESTS FOR ASSETS IN NMCI AOR STATUS SHALL BE SUBMITTED BY SITE NMCI VENDOR (EDS) PERSONNEL TO THE SUPPORTED LOCAL MARINE CORPS ORGANIZATION.

2. MARINE CORPS ORGANIZATIONS. MARINE CORPS ORGANIZATIONS SHALL SUBMIT POA&M REQUESTS FOR GOVERNMENT CONTROLLED ASSETS, AS WELL AS THOSE GENERATED BY THE NMCI VENDOR FOR AOR SYSTEMS UNDER THE UNIT'S PURVIEW. THESE POA&M REQUESTS WILL BE SUBMITTED TO THE MCNOSC VMT VIA THE NETOPS REPORTING STRUCTURE.

3. DEPLOYED UNITS. FOR OFFICIAL IAVM RELATED OPERATIONAL DIRECTIVE POA&MS, DEPLOYED UNITS SHALL SUBMIT REQUESTS TO THE SAME ENTITY AS WHEN IN GARRISON. AS APPROPRIATE, PARENT ORGANIZATIONS WILL FORWARD REQUESTS TO THE MCNOSC VMT. ALTHOUGH A POA&M MAY BE GRANTED BY THE MCEN DAA, COCOMS MAY OVERRIDE THAT DECISION AND REQUIRE COMPLIANCE WITH THE ORIGINAL DEADLINE.

(E) POA&M REQUEST CONTENT. POA&MS WILL ONLY BE ACCEPTED FOR REVIEW IF COMPLETED USING THE MOST CURRENT POA&M TEMPLATE

LOCATED ON THE VMT SIPRNET WEB SITE LISTED BELOW. ADDITIONALLY, POA&M REQUESTS WILL NOT BE PROCESSED UNLESS ALL INFORMATION REQUIRED IN THE TEMPLATE IS PROVIDED. POA&M REQUESTS THAT DO NOT ADDRESS HOW ASSETS WILL BE PROTECTED UNTIL PATCHED WILL BE DISAPPROVED. SPECIFIC ASSETS MUST BE IDENTIFIED IN THE POA&M REQUEST BY MACHINE NAME AND IP ADDRESS. A COMPLETE SCAN OF EACH ASSET MUST BE PROVIDED WITH THE POA&M. THE SCAN MUST BE NO OLDER THAN 14 DAYS.

(F) ENDORSEMENT OF POA&M REQUESTS. MARFORS MAY EITHER ENDORSE AND FORWARD A POA&M REQUEST TO THE MCNOSC FOR FURTHER CONSIDERATION, OR THEY MAY DISAPPROVE IT. DISAPPROVED REQUESTS SHALL NOT BE SUBMITTED TO THE MCNOSC.

(G) METHOD OF SUBMISSION. POA&M REQUESTS SHALL BE SUBMITTED TO THE MCNOSC VIA OPDRS. IF THIS CAPABILITY IS INOPERABLE, EMAIL SUBMISSION TO THE MCNOSC VMT PER PARA 6 BELOW.

(H) POA&M APPROVAL AUTHORITY. SOLE AUTHORITY TO APPROVE POA&M REQUESTS WITHIN THE MARINE CORPS RESTS WITH THE MCEN DAA.

F. COMPLIANCE VERIFICATION.

(1). ENTERPRISE COMPLIANCE VERIFICATION. PER REF I, THE MCNOSC, AS THE USMC COMPUTER NETWORK DEFENSE SERVICE PROVIDER, IS REQUIRED TO PERIODICALLY VERIFY COMPLIANCE WITH IAVM OPERATIONAL DIRECTIVES AND CTO 08-05 VULNERABILITY SCANNING. AT A MINIMUM, THE MCNOSC WILL CONDUCT MONTHLY SAMPLINGS OF THE MCEN (BOTH NON-NMCI AND NMCI) THROUGH VULNERABILITY ASSESSMENTS. THE VMT WILL CONDUCT TARGETED RETINA SCANS OR WILL DIRECT COMMANDS TO CONDUCT SCANS TO VALIDATE COMPLIANCE INFORMATION REPORTED TO OPDRS. REGIONAL BLUE AND GREEN TEAMS WILL ALSO CONDUCT VULNERABILITY SCANS AS REQUIRED OR AS DIRECTED BY THE VMT. NOTED DISCREPANCIES SHALL BE REPORTED TO THE MCEN DAA, AND MCNOSC VMT. AS APPROPRIATE, DISCREPANCIES WILL BE REPORTED TO DIRECTOR C4 FOR ACTION. THE MCEN DAA, MCNOSC VMT, THE AFFECTED CAR/G-6, AND THE NON-COMPLIANT ORGANIZATION WILL THEN WORK TOGETHER TO RESOLVE THE ISSUE.

(2) LOCAL COMPLIANCE VERIFICATION

(A) SCANNING: SECURE CONFIGURATION COMPLIANCE VERIFICATION INITIATIVE (SCCVI) TOOLS HAVE BEEN PROCURED BY DOD FOR ENTERPRISE USE TO ASSIST IN VULNERABILITY ASSESSMENTS. EYE RETINA IS THE APPROVED DOD TOOL FOR NETWORK SCANNING. HOWEVER, COMMANDS ARE ENCOURAGED TO USE ALTERNATIVE DAA APPROVED SCANNING TOOLS FOR VERIFICATION ALONG WITH RETINA.

(B) ALL COMMANDS ARE REQUIRED TO APPOINT IN WRITING GREEN TEAM MEMBERS. PER REF I, THESE INDIVIDUALS MUST BE PROVIDED THE OPPORTUNITY TO RECEIVE THE REQUISITE IA TOOLS TRAINING. COMMAND IAMS MUST THEN SUBMIT THE NAME OF INDIVIDUALS TO HQMC C4 IA TO RECEIVE TIER 4 ADMINISTRATOR ACCOUNTS ON THE MCEN. TIER 4 ACCOUNTS WILL ALLOW GREEN AND BLUE TEAMS WITH THE APPROPRIATE PRIVILEGES TO PERFORM THE ASSESSMENTS.

(C) REMEDIATION: SECURE CONFIGUATION REMEDIATION INITIATIVE (SCRI) TOOL HAS ALSO BEEN PROCURED BY DOD. HERCULES BY MCAFEE IS THE AUTHORIZED TOOL FOR REMEDIATION. COMMANDS ARE AUTHORIZED TO USE OTHER DAA APPROVED TOOLS FOR REMEDIATION PURPOSES.

(D) ALL VULNERABILITY ASSESSMENTS WILL BE CONDUCTED IAW REF J.

G. THE MCNOSC VMT WILL COMPILE AND SUBMIT AN AGGREGATED SERVICE REPORT OF IAVM COMPLIANCE AND EXTENSIONS TO THE JTF-GNO. THIS SHALL BE ACCOMPLISHED BY THE JTF-GNO SPECIFIED DEADLINE.

6. IAVM NON-COMPLIANCE. MCEN DAA AUTHORITY TO OPERATE ANY SYSTEM, DEVICE, OR NETWORK SEGMENT ON THE MCEN IS CONTINGENT UPON OPERATIONAL DIRECTIVE COMPLIANCE. THEREFORE, NON-COMPLIANT SYSTEMS ARE SUBJECT TO A DENIAL OF AUTHORITY TO OPERATE (DATO). THIS MAY RESULT IN IMMEDIATE PHYSICAL REMOVAL FROM THE MCEN OR BE BLOCKED FROM NETWORK COMMUNICATIONS PENDING CORRECTION OF THE NON-COMPLIANT STATUS.

7. USMC COMMANDS WILL SUPPORT THE JTF-GNO DIRECTED ENHANCED

COMPLIANCE VALIDATION (ECV) PROCESS. AN ECV IS AN ASSESSMENT METHODOLOGY THAT EXPANDS UPON THE ORIGINAL NIPRNET AND SIPRNET COMPLIANCE VALIDATIONS AS MANDATED IN THE CJCSI 6211.02B. THE ECV PROGRAM IS A PART OF THE PERSISTENT PRESENCE OF FRIENDLY FORCES ON THE GLOBAL INFORMATION GRID (GIG), PROVIDING A QUICK LOOK AT COMPLIANCE TO DOD IA POLICIES AND GUIDELINES. FOR ADDITIONAL INFORMATION REGARDING THIS MATTER, CONTACT THE VULNERABILITY MANAGEMENT TEAM AT COMM 703-784-5300, DSN 278-5300, OR BY SENDING EMAIL TO MCNOSCVMT@MCNOSC.USMC.MIL (LISTED IN THE MCEN GAL AS MCNOSC VMT).

8. RESERVE APPLICABILITY. THIS BULLETIN IS APPLICABLE TO THE MARINE CORPS TOTAL FORCE AND CONTRACTORS IN SUPPORT OF THE MARINE CORPS.

10. CANCELLATION CONTINGENCY. THIS BULLETIN, UNLESS SUPERCEDED, IS CANCELLED 01 NOVEMBER, 2009.

11. RELEASE AUTHORIZED BY BGEN G. J. ALLEN, DIRECTOR, COMMAND, CONTROL, COMMUNICATIONS, AND COMPUTERS/CHIEF INFORMATION OFFICER OF THE MARINE CORPS.//