

FROM:DA WASHINGTON DC//SAIS-IAS//

TEXT

:UNCLAS

SUBJECT: NETWORK SECURITY IMPROVEMENT PROGRAM (NSIP): ARMY POLICY FOR THE IMPLEMENTATION OF THE INFORMATION ASSURANCE VULNERABILITY (IAVA) PROCESS.

REFERENCE:

A. SECDEF MESSAGE DTG 252016ZJUN98, SUBJECT: INFORMATION ASSURANCE VULNERABILITY ALERT PROCESS

B. SAIS-IAS MESSAGE DTG 271633Z MAY 98, SUBJECT: IMPLEMENTING INFORMATION ASSURANCE (IA) VULNERABILITY ALERT/POSITIVE CONTROL IN SUPPORT OF ARMY COMPUTER NETWORK DEFENSE

1. THE PURPOSE OF THIS MESSAGE IS TO CLARIFY AND EXPAND ARMY POLICY FOR THE IAVA PROCESS. THIS POLICY APPLIES TO THE ACTIVE ARMY, THE ARMY NATIONAL GUARD, AND THE U.S. ARMY RESERVE.

2. REFERENCE A. ABOVE PROMULGATED DOD POLICY FOR IMPLEMENTING IAVA. THIS MESSAGE TASKED EACH SERVICE WITH ESTABLISHING "POSITIVE CONTROL" OVER THEIR SYSTEMS AND NETWORKS. AS STATED IN REFERENCE B. ABOVE, THE CHIEF INFORMATION OFFICER (CIO) OF THE ARMY IS RESPONSIBLE FOR EXECUTING "POSITIVE CONTROL" BY ENSURING A MEANS FOR (1) VULNERABILITY IDENTIFICATION, DISSEMINATION, AND ACKNOWLEDGMENT; (2) COMPLIANCE REPORTING; AND (3) COMPLIANCE VERIFICATION. THE CIO IS DESIGNATED AS THE ARMY POC TO ACKNOWLEDGE RECEIPT (WITHIN FIVE DAYS) OF DEFENSE INFORMATION SYSTEMS AGENCY (DISA) ISSUED IAVA MESSAGES, TO AGGREGATE COMPLIANCE AND WAIVER DATA, AND TO REPORT THE SERVICE STATUS TO DISA. IN ADDITION, THE ACERT/CC AGGREGATES MACOM/PEO/PM COMPLIANCE REPORTING DATA ON ALL IAVA MESSAGES AND PROVIDES REPORTS TO THE ODISC4 ARMY IA OFFICE, THE ARMY CIO AND ARMY SENIOR LEADERSHIP.

3. THE CIO OF THE ARMY (THE DIRECTOR OF INFORMATION SYSTEMS FOR

COMMAND, CONTROL, COMMUNICATIONS, AND COMPUTERS [DISC4]), AND THE ARMY DEPUTY CHIEF OF STAFF FOR OPERATIONS AND PLANS (DCSOPS) DESIGNATED THE LAND INFORMATION WARFARE ACTIVITY'S (LIWA) ARMY COMPUTER EMERGENCY RESPONSE TEAM COORDINATION CENTER (ACERT/CC) AS THE ARMY'S FOCAL POINT FOR IMPLEMENTATION OF THE IAVA PROCESS.

4. ACERT/CC ISSUES ALERTS AND ADVISORIES VIA THE ACERT/CC LISTSERV ON BEHALF OF THE CIO AND THE DCSOPS OF THE ARMY. TO PROVIDE REDUNDANCY, IAVA ALERTS AND ADVISORIES ARE ALSO DISSEMINATED VIA GENERAL SERVICE (GENSER) MESSAGE AND THE ODISC4 IA EMAIL DISTRIBUTION LIST. THESE MESSAGES ARE BASED ON BOTH MANDATORY DISA ISSUED IAVA MESSAGES AND ARMY GENERATED IAVA REQUIREMENTS. ACERT/CC IAVA MESSAGES DIRECT SPECIFIC ACTIONS AND GIVE MANDATORY SUSPENSE DATES FOR COMPLIANCE. IF A MACOM/PEO/PM CANNOT MEET THE SUSPENSE FOR COMPLIANCE, THEY MUST CONTACT THE ACERT/CC, COORDINATE A PLAN, AND SET A NEW DATE FOR COMPLIANCE. THE PLAN MUST PROVIDE A MIGRATION PATH WITH MILESTONES FOR A SECURITY SOLUTION APPROVED BY THE APPROPRIATE MACOM/PEO/PM DESIGNATED APPROVING AUTHORITY (DAA), AND THE PLAN MUST BE FORWARDED TO THE CIO OF THE ARMY (SEE ODISC4 POCS IN PARA 12) FOR APPROVAL. THE ACERT/CC, ON BEHALF OF THE ARMY CIO, MAY GRANT AN EXTENSION, BUT THE MACOM/PEO/PM DOES NOT HAVE THE OPTION OF NOT REPORTING ACKNOWLEDGEMENT AND COMPLIANCE. NOTE: THE CIO OF THE ARMY IS THE FINAL APPROVING AUTHORITY OF MIGRATION PLANS TO IMPLEMENT IAVA MESSAGES.

5. IT IS MANDATORY THAT ALL SYSTEMS ADMINISTRATORS, INFORMATION ASSURANCE/INFORMATION SYSTEM SECURITY PERSONNEL, NETWORK OPERATIONS PERSONNEL, AND FORCE PROTECTION PERSONNEL SUBSCRIBE TO THE ACERT/CC LISTSERV. THESE PERSONNEL CAN SUBSCRIBE TO THE LISTSERV VIA THE ACERT/CC WEBSITE SITE ([HTTP://WWW.acert.1stiocmd.army.mil](http://www.acert.1stiocmd.army.mil)). WHILE THE ACERT/CC LISTSERV IS THE OFFICIAL NOTIFICATION FOR IAVA COMPLIANCE REQUIREMENTS TO MACOM/PEO/PM LEVEL IAOS, IT IS INFO TO SUBORDINATE ELEMENTS UNTIL TASKED IN ACCORDANCE WITH (IAW) PROCEDURES ESTABLISHED BY THE MACOM/PEO/PM. LIKewise, COMPLIANCE REPORTING WILL BE ACCOMPLISHED IAW MACOM/PEO/PM IAVA PROCEDURES. THE MACOM/PEO/PM INFORMATION ASSURANCE OFFICER (IAO) WILL REPORT THE COMMAND'S ACKNOWLEDGEMENT AND COMPLIANCE STATUS TO THE ACERT/CC.

6. THE INFORMATION ASSURANCE (IA) OFFICER FOR EACH MACOM/PEO/PM IS RESPONSIBLE FOR:

A) REPORTING THE ACKNOWLEDGEMENT OF THE IAVA MSG TO THE ACERT/CC, USUALLY WITHIN 5 DAYS.

B) PROVIDING THE COMMANDER'S GUIDANCE TO SUBORDINATE UNITS/ORGANIZATIONS/ACTIVITIES/ELEMENTS/PROGRAMS AND ENSURING THE MACOM/PEO/PM CHAIN OF COMMAND IA OFFICERS COMPLY WITH IAVA REQUIREMENTS.

C) REPORTING MACOM/PEO/PM COMPLIANCE STATUS. BOTTOM LINE: THE MACOM/PEO/PM IA OFFICER IS RESPONSIBLE FOR REPORTING THE COMMAND'S IAVA ACKNOWLEDGEMENT AND COMPLIANCE STATUS TO THE ACERT/CC.

D) ENSURING INSTALLATION/UNIT IA OFFICERS AND INSTALLATION/UNIT SYSTEM ADMINISTRATORS/NETWORK MANAGERS COORDINATE WITH PEOS/PMS PRIOR TO TAKING ACTION ON ALERTS THAT ADDRESS VULNERABILITIES ON PLATFORMS UNDER PEO/PM COGNIZANCE.

7. FOR NOCS AND CERTS ONLY: IF AN ATTACK TARGETS SERVERS AND THE NEED FOR A QUICK DISSEMINATION/RESPONSE NEGATES THE UTILITY OF GENSER MESSAGES, AN ADDITIONAL MEANS FOR DISSEMINATION MUST BE AVAILABLE. ALL ARMY NETWORK OPERATION CENTERS (NOC) AND ARMY COMPUTER EMERGENCY RESPONSE TEAMS (CERTS) MUST MAINTAIN A DATABASE THAT WILL PROVIDE THE NOCS AND CERTS THE ABILITY TO CONTACT KEY NOC AND CERT PERSONNEL TELEPHONICALLY. THIS WILL BE THE PRIMARY BACK-UP FOR DISSEMINATION OF IAVA INFORMATION.

8. COMMANDERS/DIRECTORS AT ALL LEVELS ARE RESPONSIBLE FOR THE ACCURACY OF THEIR IAVA REPORTING FOR ENSURING THAT ALL SUBORDINATE UNITS RECEIVE THE IAVA INFORMATION, THAT THE DIRECTED "FIX" IS IMPLEMENTED, AND THAT THE MACOM/PEO/PM COMPLIANCE STATUS IS REPORTED TO THE ACERT/CC AS OUTLINED IN PARAGRAPH 5, THIS MESSAGE.

9. MACOMS/PEOS/PMS HAVE THE OPTION OF ALLOWING THE ACKNOWLEDGEMENT AND COMPLIANCE FOR THEIR SUBORDINATE UNITS TO BE REPORTED VIA ANOTHER MACOM WHEN THE SUBORDINATE UNITS ARE LOCATED IN A GEOGRAPHICALLY SEPARATED LOCATION.

A) HOWEVER, THE MACOM/PEO/PM MAY NOT DELEGATE THE

ACKNOWLEDGEMENT AND COMPLIANCE RESPONSIBILITIES OF THEIR SUBORDINATE ELEMENTS.

B) SUBORDINATE ELEMENTS IN A GEOGRAPHICALLY SEPARATED AREA MAY HAVE THEIR COMPLIANCE AND REPORTING INFORMATION ROLLED UP INTO THEIR HOST'S SITE REPORT ONLY AFTER THERE HAS BEEN MACOM/PEO/PM IAO TO MACOM/PEO/PM IAO COORDINATION AND AGREEMENT ON HOW THE ACKNOWLEDGEMENT AND COMPLIANCE DATA WILL BE REPORTED TO THE ACERT/CC.

10. PEOS/PMS HAVE THE SAME RESPONSIBILITIES THAT A MACOM HAS TO REPORT ACKNOWLEDGEMENT AND COMPLIANCE STATUS FOR ALL SUBORDINATE UNITS/ELEMENTS/ACTIVITIES/PROGRAMS WITHIN THEIR LIFE CYCLE SUPPORT AUTHORITY.

A) PEOS/PMS MUST ENSURE THAT SUBORDINATE UNITS/ELEMENTS/ACTIVITIES/PROGRAMS MAINTAIN A CONFIGURATION BASELINE ON SYSTEMS FOR WHICH THEY HAVE POST PRODUCTION SOFTWARE SUPPORT (PPSS) RESPONSIBILITIES.

B) THE PEO/PM IS RESPONSIBLE FOR COMPARING IAVA MESSAGES AGAINST SYSTEM BASELINES AND TAKING APPROPRIATE ACTION TO ENSURE THE SYSTEM MEETS THE IAVA DIRECTED STANDARD.

C) NO PEO/PM HAS A WAIVER THAT EXEMPTS FIELDDED/IN DEVELOPMENT SYSTEMS FROM MEETING IAVA STANDARDS. IF A SYSTEM CANNOT MEET THE IAVA STANDARD WITHIN THE SUSPENSE, THEN A WAIVER MUST BE SENT TO THE ODISC4 POC THIS MESSAGE. IN ORDER TO CONSIDER THE WAIVER, A MIGRATION PLAN WITH MILESTONES THAT OUTLINES HOW THE SYSTEM WILL MEET THE IAVA REQUIREMENT MUST BE ATTACHED.

D) THE PEO/PM IS ALSO RESPONSIBLE FOR ENSURING THAT THE IAVA MESSAGES ARE DISSEMINATED TO ALL UNITS/ELEMENTS/ACTIVITIES/PROGRAMS THAT ARE DEVELOPING SYSTEMS AND ENSURE THAT IAVA DOCUMENTED VULNERABILITIES ARE CORRECTED PRIOR TO FIELDING.

11. TO MEET THE DEPUTY SECRETARY OF DEFENSE (DEPSECDEF) IAVA "POSITIVE CONTROL" COMPLIANCE REPORTING REQUIREMENTS, ALL MACOM/PEO/PM IAOS MUST ENSURE THAT SUBORDINATE IAOS AT EVERY ECHELON MAINTAIN A COMPLETE "LIST" (A DATABASE, SPREADSHEET, ETC) OF ALL SYSTEM ADMINISTRATORS AND NETWORK MANAGERS RESPONSIBLE TO THEM FOR IMPLEMENTING MANDATORY IAVA REQUIREMENTS, INCLUDING THEIR EMAIL

ADDRESSES AND PHONE NUMBERS. WHILE THERE IS NO REQUIREMENT FOR MACOM/PEO/PM IAOS TO "ROLL UP" ALL DATA INTO A "MASTER LIST" FOR THE COMMAND, MACOM/PEO/PM IAOS MUST HAVE THE CAPABILITY TO QUERY EVERY SUBORDINATE IAO AND RECEIVE THEIR "LIST." HQDA IS AWAITING ADDITIONAL IAVA REPORTING GUIDANCE FROM THE OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE FOR COMMAND, CONTROL, COMMUNICATIONS, AND INTELLIGENCE (OASDC3I) AND ANTICIPATES "POSTIVE CONTROL" COMPLIANCE REPORTING WILL INCLUDE BOTH THE NUMBER OF SERVERS AFFECTED AND THE NUMBER IN COMPLIANCE FOR WHICH SYSTEMS ADMINISTRATORS ARE RESPONSIBLE. ADDITIONAL INFORMATION WILL BE PROVIDED AS IT BECOMES AVAILABLE. THIS PROCESS AND/OR DATABASE MUST BE OPERATIONAL NLT 15 OCT 99.

12. DISC4 POLICY POCS FOR THIS MESSAGE ARE LTC ROY LUNDGREN, DSN: 664-8377, COM 703-706-8377, EMAIL LUNDGL@HQDA.ARMY.MIL OR PHILLIP LORANGER, DSN: 327-5887, COM 703-607-5887, EMAIL LORANPJ@HQDA.ARMY.MIL. TECHNICAL POLICY POCS FOR THIS MESSAGE ARE RON STURMER, DSN 664-6870, COM 703-604-6870, EMAIL: STURMRT@HQDA.ARMY.MIL; RALPH A. LOWENTHAL, DSN 327-5886, COM 703-607-5886 EMAIL LOWENRA@HQDA.ARMY.MIL.