SUBJECT: Clarification of Procedures for Operational Test and Evaluation of Information Assurance in Acquisition Programs

DOT&E memorandum of January 21, 2009, Procedures for Operational Test and Evaluation of Information Assurance in Acquisition Programs, provides guidelines for verifying the effectiveness of information assurance (IA) and computer network defense (CND) measures in acquisition programs during operational test and evaluation events. I expect these guidelines to be adhered to for programs that exchange information and are under DOT&E oversight. Operational Test Agencies should consider incorporating that policy into their procedures for similar programs that are not under oversight. It has come to my attention, however, that some programs have misinterpreted that memorandum to imply IA and CND testing must be done during the Initial Operational Test and Evaluation (IOT&E) period. This memorandum is to clarify that is not the case.
To be effective, IA and CND measures need to be tested as early as possible once hosted on the operational network. I encourage this testing be planned and executed in an early integrated test venue, if possible. The results of the testing should be shared to all stakeholders as soon as they are available. If a penetration test was conducted within one year, even if by another entity, the results of that test can be used in lieu of another test as long as sufficient information is available to understand the threat emulated and verify the adequacy of the test. Information from this test as well as that obtained from Developmental Test and Evaluation and Information Assurance Certification efforts must still be assessed and included in the Operational Test Agency’s IOT&E report.

To support proper planning, the Test and Evaluation Master Plan (TEMP) should clearly identify what events will support the IA and CND assessment and address the requirements in DOT&E’s memorandum of January 21, 2009. In particular, the TEMP must specifically identify the Red Team requirements for the penetration test and the required threat to be emulated. If the system is connected to a network with other systems with higher Mission Assurance Category (MAC) and Confidentiality Level (CL) than the system under test, I expect the threat emulation to be planned to the higher MAC and CL. If the threat level cannot be emulated on the operational network, the TEMP should identify what closed test network will be used and the verification and validation effort needed to ensure that network provides an operationally realistic environment.

As with all guidelines, I will consider deviations from prescribed practices on a case by case basis.

J. Michael Gilmore
Director

cc:
ASD (NII)
DDT&E