

An Enterprise Environment for Information Assurance/Computer Network Defense Testing and Evaluation

By Parker Horner, EWA Government Systems, Inc. and
Steve Moore, Booz Allen Hamilton

Information Assurance (IA) is, by its nature, an “enterprise” undertaking. Providing a developmental and operational testing environment for IA/CND is explored. For example, the environment must allow the SUT to function with: its Command and Control/Battle Management node; its Intelligence, Surveillance, Reconnaissance node; its airborne controller; the tactical unit of action, etc. And, IA must be evaluated in the operational environment(s) during the SUT lifecycle. That presents a challenge, since front-line operational assets are often not available for SUT. A persistent, distributed environment is needed.

Extending and expanding the IO Range as a department-wide enterprise solution for IA/CND Testing and Evaluation is examined. The confluence of two major themes – 1) the maturation and capability of the IO Range and 2) the need for an environment to support DOT&E policy for end-to-end IA/CND operational testing – are melded into a conceptual solution for the Department of Defense.

The paper will discuss how the IO Range functions today, its fundamental DoD mandate, its plans through 2012, and how those plans could be adjusted/adapted to absorb additional IA/CND requirements. An implementation status of IA/CND operational test policy is presented, including Industrial Committee on OT&E actions, unresolved issues, and plans. If timing and program access allow, a major system pilot SUT implementation may be discussed. Investment options, policy decisions, and customer outreach/planning initiatives that would be needed to bring this conceptual solution to a real, robust testing capability will be presented and discussed. A discussion on stakeholder (USD(I), ASD/NII, DOT&E, AT&L/DTRMC, Joint Staff J3 and J6, USD(P&R), STRATCOM, JFCOM, Services) potential equities will be presented.