Defense-wide Information Assurance Program (DIAP)

SESSION ABSTRACT

The purpose of the Defense-wide Information Assurance Program (DIAP) Panel is to introduce the audience to the mission, functions and organizational structure of the DIAP as well as to discuss some current key issues within the Department of Defense in the Information Assurance arena. These issues are: Computer Network Defense and the role of USSPACECOM in that mission, Research and Development initiatives in Information Assurance and the implementation of Public Key Encryption Infrastructure (PKI) within the Department of Defense. Prior to the panel beginning, 3x5 cards will be passed out to the audience for them to write down questions for the panel to answer after all the presentations have been made. The panel will be introduced by the panel chair, CAPT J. Katharine Burton, who will then present a 10-15 minute briefing on the DIAP. Providing time allows, a few questions may be asked and answered at this point. Following the questions, the second panelist, COL Tom Muchenthaler, from the USSPACECOM UCP 99 Activation Task Force will give a 10-15 minute presentation on the assumption of the global DoD Computer Network Defense mission and the potential impacts of that mission. Providing time allows, a few questions may be asked and answered, then the third panelist will make a presentation. Ms. McBride will provide a brief description about how the DoD plans, coordinates, integrates and oversees the Department's Information Assurance Research and Technology resources. Mr. Viola will discuss recent events pertaining to Public Key Infrastructure (PKI) within the Department as well as discuss his responsibility in pulling together all the activities that must take place simultaneously regarding this issue. He will also discuss organizations' roles and responsibilities.

When all the panelists have made their presentations, the panel chair will open up the discussion to questions from the floor. Depending on the questions, panel members will be asked for their opinion on the answer if another panelist answered the primary question. If there are insufficient questions from the floor, the questions submitted on the 3x5 card will be used to stimulate discussion among the panel members and with the audience.

PANELIST'S TOPIC: CAPT J. Katharine Burton, USN

DEFENSE-WIDE INFORMATION ASSURANCE PROGRAM

The Department of Defense is becoming increasingly dependent on a commercially-based global information over which it has little control. This dependence is heightening our exposure and vulnerability to a rapidly growing number of sophisticated internal and external cyber threats. Today's inter-networked information technologies make it possible for an adversary to influence or control many systems, networks and users by attacking a single connection to a network. Once inside a system, an adversary can exploit it and the systems networked to it. This global marriage of systems and networks creates a *shared-risk* environment and a new dimension for warfare.

Information Assurance (IA) is the means by which cyber threats are countered. IA is emerging as a critical component of the DoD's operational readiness. IA enables the systems and networks composing the Defense Information Infrastructure (DII) to provide protected, continuous and dependable service in support of both warfighting and business missions. IA relies on a blend of managerial, procedural and technical activities that work toward assured availability, integrity, authenticity, confidentiality, and non-repudiation of information services, while providing the means to efficiently reconstitute these vital services following an attack. It includes an extended focus on DoD missions and infrastructure that are substantially interwoven with out National Information Infrastructure (NII) and increasingly dependent on services derived from the Global Information Infrastructure (GII).

In January 1998, the Deputy Secretary of Defense approved the creation of the Defense-wide Information Assurance Program (DIAP) to provide for the planning, coordination, integration , and oversight of the Department's IA activities and resources. The DIAP forms the Department's core organizing element for achieving a more comprehensive, coherent and consistent IA program. It includes a process designed to give central oversight while retaining decentralized execution to realize continuous improvement in our IA posture. The DIAP's central coordination and oversight activities enable the Department to accurately develop, validate, integrate, and prioritize DoD-wide IA requirements, determine the return on our IA investments, and objectively assess our defense-in-depth efforts to protect the DII and critical elements of NII and GII. Properly constructed and executed, the DIAP process can achieve both necessary and sufficient responsiveness to current and future IA issues, threats and vulnerabilities.

PANELIST'S TOPIC: COL Tom Muchenthaler, USAF

USCINCSPACE ASSUMPTION OF CND MISSION

The Secretary of Defense directed USCINCSPACE to assume the DoD's Computer Network Defense (CND) support mission, including assumption of responsibility for the Joint Task Force for CND (JTF-CND) by 1 Oct 1999. USCINCSPACE will coordinate and direct operations to protect and defend the computer systems and networks of the Defense Information Infrastructure (DII) or other vital national security interests, as directed, against computer network attacks and intrusions. On behalf of all CINCs, Military Services, and DoD Agencies, USCINCSPACE will advocate CND policy, doctrine, mission level requirements, and operational issues to the Chairman of the Joint Chiefs of Staff.

Just as the DII is global in its nature, so must be the responsibilities and associated authorities for its defense. An attack or intrusion perpetrated in one area of the world can impact operations in other regions. Therefore, to protect and defend the DII, USCINCSPACE will be required to direct protect, response and restoral actions across the DoD. To accomplish this objective, USCINCSPACE will employ a multidimensional strategy, building upon and leveraging the DIAP and other efforts. This approach will integrate operations, planning, policy, requirements, and personnel actions to provide a layered defense responsive to varying threats. The strategy will seek to evolve current reactive processes to more predictive and proactive processes through strategic partnerships with DoD Components, other U.S. Government Agencies, the Intelligence Community (IC), allies and industry.