DOD Information Security Projections:
The Service PM Perspective

Panel Chairperson
Jim Litchko
General Manager
Integrated Management Services, Inc. (IMSI)
Arlington, VA

United States Navy
Capt Dan Galik
Program Manager
Navy Information Systems Security
SPAWAR, San Diego, CA

United States Army
COL Mike Brown
Deputy Director
DISC4, Information Assurance
Pentagon, Washington, DC

United States Air Force
Col Roger J. Robichaux
Chief of the Networks Division, Systems Directorate
AF Communications and Information Center
Pentagon, Washington, DC

The panel members are the individuals who drafted the INFOSEC maps for each of the DOD Services. During this panel presentation, they will discuss the key issues and concerns, critical paths, concepts, and which solutions will be deployed. They will address the question: “What is most important to my Service: professionals, security products, assurance tools, training, policy, or awareness?”

Captain Galik will start the panel discussion by explaining the Navy’s strategy of capitalizing on the use of PC-based COTS technology and high-capacity networking systems technology. He will present this in the reference to the Navy's "Information Technology for the 21st Century" (IT-21). Security technology is core to the fielding of IT-21, and there are many challenging issues that are being resolved as the Navy tries to incorporate modern COTS security technology into high-speed ATM networks. He will discuss how the Navy will use many of the same security products and solutions that are being used in private industry. The Navy's security strategy is based on a "defense in depth" concept. This acknowledges that no single security product, by itself, addresses all the security threats and risks that our warfighting systems face today.

Col Brown is the Deputy Director of the Information Assurance for the Army staff in the Pentagon. He will explain the Army’s position that personnel must understand their responsibilities and are held responsible for their actions. Key to the Army’s plan, is to ensure that their personnel are trained in their security duties and the security capabilities of their computer and network systems. During his presentation, he will refer to the successful integration of network assurance tools and reporting initiatives that the Army used to secure the systems in the 1997 Division XXI exercises. Col Brown will also describe their pro-active initiatives in deploying intrusion detection systems to critical army systems, establishing theater CERT operations, and providing Army commands with a list of approved firewalls, a IDS, and a multilevel secure (MLS) guard.

Col Robichaux provides the planning, policy, architectures, process and systems management expertise for implementation, operations and modernization of AF information systems and networks. His division also provides the technical review of implementation plans and technical solution requirements for base communications infrastructure and Information Protect and Information Assurance policy, guidance, strategy, capabilities and program oversight. Col Robichauz will talk about the Air Force's key communications and information initiatives. He will explain how these directly support and act as force multipliers in support of the six core competencies of Global Engagement: Air and Space Superiority, Global Attack, Rapid Global Mobility, Precision Engagement, Information Superiority, and Agile Combat Support. One key initiative to standardize Air Force networks and institutionalize networking skills as a communications core competency, is the Operationalizing and Professionalizing the Network (O/PTN) concept. The term "operationalizing" focuses on the command and control structure of network operations. It consists of Design Operational Capability (DOC) taskings, Status Of Resources and Training System (SORTS) reporting, inspections and evaluations, graduated response, and operational reporting. "Professionalizing" networks involves actions required to organize, train, equip, and sustain the networks and personnel who operate them. Specific initiatives include applying engineering rigor to garrison and deployed networks, designing layered "information protection" throughout the network, certifying and licensing networking professionals and users, and standardizing network equipment based on a common Air Force technical architecture."

Each member of the panel will present an overview of their Services' plans and strategies and their projection of the major challenges in implementing their plans over the next five years. The audience will have then have time to ask questions of the panel.