What about I^{3} - INFOSEC Integration Issues: "What worked, did not work, and why?"

Jim Litchko
General Manager
IMSI

Jim Brenton, CISSP
Principal Network Security Program Manager
Sprint Corporate Security

Richard Lee Doty, CISSP
Asst Exe Dir Systems Surety Division
ManTech International Corp. .

LtCol Fred W. Peters, USAF
Director, Operations/ATIC
OASD (Health Affairs) and TMA

David J Wilson
Information Assurance Product Manager
Telos Corp. .

With over 100 years of combined experience, this panel will discuss the successes and failures with integrating security and certifying operational and evolving information systems in both government and commercial sectors. “What worked, did not work, and why” will be presented using real-world case studies in this panel discussion. Each of the panelists will provide different perspectives and approaches to solving information systems security problems - tools by which the audience can approach their specific problems in the future.

Richard Doty has over 23 years of experience in personnel, physical, technical, operations, and computer security. Richard has experience in integrating these disciplines into cohesive “security programs.” Currently, he is the contract lead for the effort to re-write the security architecture for the Department of State. Richard has over seven years experience in addressing computer security issues for both federal and local government. He will discuss the need to integrate personnel and physical security through durable policy and regulation to any information security solution; to develop well-written and durable policy and regulation so users and managers have a formal standard against which they should be held and measured; and to implement good physical security, so your information system security can not be easily circumvented. The bottom line is that security must be integrated as a “program” vice a disjointed mob of single issues - and it must be a program that senior management is willing to support.

David Wilson has over 11 years of security engineering experience as a consultant to the US military community and civilian federal Government agencies. Areas of experience include certification & accreditation (C&A) and systems engineering for C4I systems. Currently with Telos, David is developing Information Assurance solutions. responsible for managing security projects for DoD and commercial customers. David will talk about why he believes that DoD program managers have not achieved accreditation status on their networks. Many reasons include the lack of management support (i.e., C&A package seen as shelfware instead of a truly viable set of change management and contingency/disaster recovery planning resources). Also, the DITSCAP process intimidates some agencies. He will explain how the DITSCAP process can be demystified by breaking down the components requested and determining their relevance to the subject information system. David will also talk about how product evaluation status affects the status of system's accreditation and upgrades (i.e., Microsoft's Windows NT product, DoD's chosen standard network operating system (NOS), failing to achieve TPEP certification).

Jim Brenton is a Principal Network Security Program Manager for Sprint Corporate Security where he directs information and network security programs for the Government Services Division. He ensures that government security requirements are identified and met in network architectures and system specifications for full life-cycle development process of multi-tiered, distributed systems for military and civil government agencies. His background includes 23 years as an INFOSEC program manager for the US Air Force, National Security Agency, and Johns Hopkins University. Jim will discuss the issues and concerns that he has seen while implementing security within information systems, specifically: the security activities across the full life-cycle system development process, risk assessment and security policy challenges for multi-tiered, multi-vendor, distributed client/server system environments; the security testing, evaluation, and analysis for system certification and accreditation; and, the challenges of providing security awareness and training for diverse groups of non-technical users and IT professionals.

LtCol Peters has more than 16 years of information management and information technology experience. He is currently the Military Health System (MHS) Security Program Manager and principal advisor to the MHS Chief Information Officer, the Executive Director, TRICARE Management Activity (TMA), and the Assistant Secretary of Defense (Health Affairs) on matters pertaining to automation. Over the past two years, LtCol Peters developed and implemented the first enterprise wide Medical Information Systems Security Program. He brings a system manager’s and operator’s perspective to implementing security in deployed systems. His approach to gaining the C&A of over 90 healthcare systems world-wide using certification references over his security web-site has proven very successful in ensuring that his systems protect sensitive patient information.

This panel is an issues and solutions focused panel. Each member has been tasked with presenting solutions that provide the audience the opportunity to look at security problem from a difference perspective and to leave with additional solutions in their “INFOSEC Toolkit”

Chairperson's Background:

Jim Litchko

Mr. Litchko is a senior information systems security specialist with over twenty-five years experience assessing and developing information system security (INFOSEC) solutions for computer and network systems. Currently, he is General Manager for Integrated Management Services, Inc. (IMSI). He has been a senior executive for special projects and business development at the two largest commercial INFOSEC companies, Secure Computing Corporation and Trusted Information Systems, and the enterprise integrator, Telos, all internationally known for advance INFOSEC R&D, consulting, and network security products. During his twenty-year career as a Navy cryptologist, he spent his first six years supporting operations on naval combatants and air reconnaissance platforms in the Atlantic, Pacific, and European theaters. As the INFOSEC Officer on the European Command (EUCOM) Staff and U.S. Representative to the NATO INFOSEC Committees, he was responsible for INFOSEC interoperability for joint and combined operations in Europe, Africa, and the Mid-East. During his tour, he designed and deployed a unique over-the-air-rekeying communications security (COMSEC) key distribution system for CINC Europe (CINCEUR) crisis and contingency operations. This system was adopted in 1986 as the standard for joint crisis and contingency operations by JCS and was one of the initial conceptual implementations of a public key infrastructure (PKI). Mr. Litchko's last five years in the Navy were in staff and technical positions in the National Security Agencies (NSA) INFOSEC Directorate and the National Computer Security center (NCSC). He organized and executed the 1989 Joint Multi-level Security Initiative, which included security reviews of 12 Commander-in-Chiefs (CINCs) C3I systems; validated the Joint MLS requirement; and developed the NSA $18 million a year Department of Defense MLS program. He retired in 1990 as the Staff Chief for the Director of the NCSC. Since 1995, he has been an instructor for systems and network security for Johns Hopkins University, MIS Training Institute and the National Cryptologic School. He also provided INFOSEC presentations for Congressional staffs, Gartner Group, Conference Board, Price Waterhouse, Exxon, Freddie Mac, National Industrial Security Association, Computer Security Institute (CSI), National Computer Security Association (NCSA), Defense Intelligence University, and Armed Forces Communications and Electronic Association (AFCEA). Mr. Litchko has chaired panels and provided INFOSEC presentations at national and international conferences and executive conferences. He holds a Masters degree in Information Systems from John Hopkins University and a Bachelors degree in Industrial Technology from Ohio University.