The Secret and Below Interoperability (SABI) Process
Assessing Community Risk

Lt Col Mark S. Loepker, National Security Agency, Moderator
Curtis Dukes, National Security Agency
Charles Schreiner, National Security Agency
Willard Unkenholz, National Security Agency
Dallas Pearson, National Security Agency
Jack Eller, Defense Information Systems Agency

Abstract:

SABI is an Assistant Secretary of Defense for Command, Control, Communications and Intelligence (ASD/C31) mandated, Joint Chiefs of Staff, Command, Control, Communications and Computer Systems (JS/J6) sponsored Information Assurance initiative which improves the security posture of all secret and below DoD systems because it utilizes a community-based risk acceptance approach, uses proven information systems engineering principles and encourages the reuse of proven information security solutions.

The goal of SABI is to ensure secure secret and below interoperability solutions for the warfighter within community-acceptable risks. It is a network-centric process with procedures to review interconnections and leverage proven solution reuse. It is founded on information system security engineering (ISSE) principles whereby information systems security (INFOSEC) is integrated as a part of systems engineering and systems acquisition processes, strong customer participation in support of mission needs, and the optimal use of INFOSEC disciplines to provide security solutions. Documentation implements the DoD Instruction 5200.40, Defense Information Technology Security Certification and Accreditation Process (DITSCAP).

The SABI process teams the local site customer with appropriate engineering, risk, vulnerability, training and programmatic community risk-focused support necessary to develop the right solution for the customer's SABI requirement. SABI maintains this community team throughout the system security engineering process. This strengthens the community risk acceptability of a specific site solution through continued dialog and participation of all relevant stakeholders.

The panel will discuss the SABI process, progress, and lessons learned as a model for engineering community risk-focused solutions.

Panel Member Background

Lt Col Mark S. Loepker is the Chief, Military Requirements Analysis Branch, Warfighter INFOSEC Support Division, National Security Agency. He is responsible for all matters impacting collection, analysis and support of military INFOSEC requirements with an emphasis on the warfighting Commander-in-Chiefs (CINC). In this capacity, Lt Col Loepker leads the Secret and Below

Interoperability (SABI) project. He last served with the Command, Control, Communications and Computer Systems Directorate, U.S. European Command, as Chief, Information Systems Security Division, responsible for all European theater policy and policy enforcement concerning information warfare and communications and computer security. During his tour he led INFOSEC actions in support of Operation Provide Comfort, Joint Endeavor and Combined Endeavor (Partnership for Peace).

Curtis W. Dukes is the Deputy Chief, Architectures and Applications Division of the Systems and Network Attack Center, National Security Agency. He is responsible for the technical direction of the Intrusion Detection and Enterprise Management System's vulnerability research within the Center. In this capacity, he leads the Joint Vulnerability Assessment Process of the Secret and Below Interoperability (SABI) Initiative. He previously served in an Intelligence Community assignment in the Directorate of Operations, Central Intelligence Agency.

Chuck Schreiner is Deputy Chief of NSA's Security Architecture and Standards Division, responsible for developing, documenting, expanding and maintaining the Network Security Framework (NSF) for the U.S. Government, and developing reusable solutions that address problems identified by the NSA customer support organization. Mr. Schreiner is currently the lead for the SABI System Security Engineering Support (SSES) effort. He also recently completed a tour as the NSA INFOSEC Representative to the Department of Defense at the Pentagon.

Willard Unkenholz is a Technical Director for the System Security Guidance and Evaluation Division, National Security Agency. His current duties involve developing and leading the DoD risk analysis capabilities applied to the Secret and Below Interoperability Initiative.

Dallas Pearson is the Technical Director of NSA's Office of INFOSEC Customer Support Services. All of Dallas' 27 years at NSA have been in technical roles in COMSEC and INFOSEC. He received a Bachelor of Science in Physics from the University of Southern Mississippi in 1970 and a Master of Science in Systems Engineering from Johns Hopkins University in 1995. He is a co-author of NSA's Information Systems Security Engineering (ISSE) Handbook and teaches an in-house introduction to ISSE course. His most recent risk-related task was re-engineering the INFOSEC Risk Analysis services of NSA.