The Secret and Below Interoperability (SABI) Process

Continuing the Discovery of Community Risk

Mark Loepker, National Security Agency, Moderator
Curtis Dukes, National Security Agency
Charles Schreiner, National Security Agency
Willard Unkenholz, National Security Agency
Corky Parks, National Security Agency
Dallas Pearson, National Security Agency
Warner Brake, Defense Information Systems Agency

Abstract:

Secret and Below Interoperability (SABI) is an Information Assurance initiative mandated by the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (ASD/C3I) and sponsored by the Joint Chiefs of Staff, Command, Control, Communications, and Computer Systems (JS/J6). SABI improves the security posture of all secret and below DoD systems by using a community-based risk acceptance approach. SABI utilizes proven system security engineering to address the risks to the community, and employs mission-oriented risk management in making sound community decisions.

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.

During the discussion about the current status of the SABI program, the panel will focus on the progress and impact of the National Information Assurance Certification and Accreditation Process (NIACAP), NSTISSI 1000.

<u>Panel Member Profiles</u>

Mark Loepker is the Chief, Information Assurance Process Special Project Office, Information Assurance Solutions, National Security Agency. He is responsible for all matters impacting the development, refinement, and implementation of the information assurance solution process. In this capacity, Mr. 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 this tour, he led INFOSEC actions in support of Operation Provide Comfort, Joint Endeavor, and Combined Endeavor (Partnership for Peace).

Curtis 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 the Chief of the Solution Security Analysis Division, National Security Agency, which provides customers with vulnerability analysis and test services to support their local risk decisions. He has held previous positions as NSA Representative to the Pentagon, Technical Director for Fielded Systems, and Deputy Chief of the RF Communications Division.

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.

Corky Parks is a risk analyst in the System Security Guidance and Evaluation Division, National Security Agency. His areas of interest include the theory and practice of information risk management, and decision theory.

Dallas Pearson is the Technical Director for Security and Evaluations in National Security Agency’s Office of Information Assurance Solutions Deployment and Maintenance. All of Dallas’ 29 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.

Warner Brake is the Deputy Chief, Information Assurance Implementation Branch of the Information Assurance Program Management Office, Defense Information Systems Agency. He is the senior certification test director and advisor for certification team members, who perform in-depth technical certification testing and compliance validation of DISA pillar, Joint, and NATO programs. He is also responsible for the periodic review and update of DOD Instruction 5200.40, DOD Information Technology Security Connection Approval Process (DITSCAP), and the operation of the Information Assurance Support Environment information desk and website.