Title of Panel: Progress of the Best Security Practices Subcommittee

Panel Chair

James P. Craft, CISSP
Information Systems Security Officer (ISSO)
United States Agency for International Development (USAID)
1300 Pennsylvania Ave, Suite 2.12-032
Washington, DC 20523-2120
Voice: 202.712.4559
Fax: 202.216.3053
Email: jcraft@usaid.gov

Panelists -- not to exceed 4 (Names and Organizations)

Marianne Swanson Computer Specialist National Institute of Standards and Technology (NIST) 100 Bureau Drive, Stop 8930 Gaithersburg, MD 20899-8930 Voice: 301.975.3293 Fax: 301-948-0279 Email: marianne.swanson@nist.gov	Mary Schanken Senior Computer Scientist National Security Agency (NSA) Fort Meade, MD 20755 Voice: 401-854-4458 Email: schanken@nsa.gov
Marty Poch Environmental Protection Agency (EPA) Washington, DC Voice: 202.564.4912 Email: poch.martin@epa.gov	Michael T. Hovey Senior Computer Scientist Computer Sciences Corporation (CSC) 1100 Wilson Blvd, Ste. 1100 Rosslyn, VA 22209 Voice: 703.465.7386 Fax: 703.465.7193 Email: mhovey@csc.com

Session abstract

The CIO Council's Best Security Practice (BSP) project fills the security knowledge gap between episodic professional classroom training and disorganized electronic bulletin board discussion threads by providing a structured capability for all Federal IT professionals to share first-hand information regarding their security implementation experiences. Upon accessing the BSP website (http://bsp.cio.gov) users can easily obtain information most relevant to their unique needs. Users can also submit information in preformatted BSP packages. A BSP packages can include artifacts, such as checklists, briefings, and policies thereby reducing cost, improving the speed, and increasing the quality of security solutions across the Federal enterprise. A feature unique to the BSP website is the capability for users to submit comments on existing BSP packages. In this way agency-specific experiences can become core community practices. CIO Council credibility and BSP content integrity is assured through an offline interagency process that reviews and manages all BSP and feedback submissions. Potential BSP population is anticipated to exceed one hundred by mid-2001. Subsequent BSP project activities include user transaction analysis to identify

needed but unsatisfied needs, technical evaluations, and development of alternative solution delivery mechanisms.

Brief summary of panelist's topics

Marianne Swanson (Panelist)

This panelist will discuss the BSP submittal and feedback review processes.

Mary Schanken (Panelist)

The general value of website and BSPs compared to other information security knowledge resources.

Marty Poch (Panelist)

Provide a customer's view of BSPs and the experience of using them

Michael T. Hovey (Panelist)

Federal agencies and vendors alike have expressed reservations regarding the information content in a BSP including proprietary information, liability, and procurement integrity. This presentation will address those concerns and others in an informative manner with examples extracted from BSPs actually submitted.

Background of audience you are trying to attract.

This panel will appeal to all Federal IT professionals both Government and vendors. Government is interested in making more cost effective decisions and deriving greater value from a shared knowledge resource. Vendors want to offer greater competitive value to their clients. The sharing of best security practices enables the entire value chain to flow more smoothly.

Short bio of panel chair and speakers

James Craft (Panel Chair)

James P. Craft is the Information Systems Security Officer (ISSO) for the U.S. Agency for International Development (USAID). While at USAID, Mr. Craft initiated the Model Information Systems Security Program (MISSP), which was designed to collect, organize, and disseminate best security practices (BSPs) for civil departments and agencies. In October 1999, he was asked to chair the CIO Council's Security Practice Subcommittee (SPS). In support of the SPS, USAID developed a proposed program plan for a Federal BSP Program (FBSPP) along with a prototype proof-of-concept web repository (http://bsp.cio.gov). Previous to USAID, Mr. Craft was employed by SRA International, Inc., Booz Allen & Hamilton, BETAC,Inc., and the U.S. Marine Corps. He earned a Business Management degree from George Mason University in 1978. Mr. Craft has received the CIO Council's 1999 and 2000 *Technology Leadership Certificates*, the 1999 *USAID Office of Inspector General Annual Achievement Award*, and the National Security Agency's Annual *SSE-CMM Program Achievement Award* in 1999.

Marianne Swanson (Panelist)

Marianne Swanson is presently a Computer Specialist in the Computer Security Division at the National Institute of Standards and Technology (NIST). She works in the area of computer security and was the program manager for the government wide incident

handling capability, FedCIRC. She is currently Acting Chair of the Federal Computer Security Program Managers' Forum and Vice Chair of the CIO Council Security Subcommittee. She co-authored the NIST Special Publication, "Generally Accepted Principles and Practices for Securing Information Technology Systems," and the NIST Special Publication, "Guide for Developing Security Plans for Information Technology Systems."

Mary Schanken (Panelist)

Mary Schanken is a Senior Computer Scientist with the National Security Agency (NSA.) where she was the first Chief of the NSA Information Systems Security Service Center (NISSC.) She has participated in the International Common Criteria Assurance Approaches Working Group and served as government lead for the development of the Systems Security Engineering Capability Maturity Model (SSE-CMM) participating in appraisals to validate the model and its appraisal methodology. She is also a Lead Assessor and a Proficiency Test Grader for the National Voluntary Laboratory Assessment Program (NVLAP) under the National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme (CCEVS.)

Marty Poch (Panelist)

Not available.

Michael T. Hovey (Panelist)

Michael T. Hovey leads Computer Sciences Corporation's support to the Security Practices Subcommittee (SPS). As part of this effort he has been responsible for the drafting of USAID's *Proposed Plan for a Federal Best Security Practices (BSP) Program (FBSPP)* and the development of the CIO Council's BSP website (http://bsp.cio.gov). Prior to CSC, Mr. Hovey worked for Infrastructure Defense and SRA International. He has also consulted to and helped author the reports of both the President's Commission on Critical Infrastructure Protection and the Commission on Roles and Mission of the Armed Forces. Mr. Hovey holds a Masters in Business Administration from Boston University and is a recipient of the CIO Council's 2000 *Technology Leadership Certificate*.