FIPS 140-1 ENCRYPTION REQUIREMENTS
CRYPTOGRAPHIC MODULE VALIDATION PROGRAM

Panel Chair: Annabelle Lee, National Institute of Standards and Technology (NIST)

Panel Members: Ray Snouffer, NIST
Laurie Mack, Communications Security Establishment (CSE) of the Government of Canada
TBD, Federal Agency Representative

Session Abstract: Cryptographic modules are tested against requirements found in FIPS 140-1, *Security Requirements for Cryptographic Modules.* Security requirements cover 11 areas related to the design and implementation of a cryptographic module. Cryptographic module validation testing is performed using the *Derived Test Requirements for FIPS PUB 140-1* document. It lists all of the vendor and tester requirements for validating a cryptographic module, and it is the basis of testing done by the Cryptographic Modules Testing (CMT) accredited laboratories. NIST and the Communications Security Establishment (CSE) of the Government of Canada jointly manage the Cryptographic Module Validation Program (CMVP). The panel will provide information on FIPS 140-1 and discuss the CMVP. Specific topics are:

Ray Snouffer will provide an overview of FIPS 140-1 including a description of the CMVP process; the advantages of using validated cryptographic modules; the responsibilities of all the organizations, for example, vendors and laboratories, that participate in the CMVP; and a discussion of the five year review and proposed update of FIPS 140-1.

Laurie Mack is the Crypto Systems Program Manager from CSE. She will talk about the impact of FIPS 140-1 in Canada and describe the similarities and differences with the U.S. program. Laurie will also discuss CSE's role in the FIPS 140-1 program and its relationship to NIST.

Annabelle Lee will discuss all the cryptographic modules that have been validated and the FIPS 140-1 conference: *Assuring Cryptographic Security* that was held in May 1998.

The Gov't. Representative will discuss how FIPS 140-1 is applicable to their agency and the benefits associated with implementing validated cryptographic modules.