# CRYPTOGRAPHIC MODULE VALIDATION PROGRAM: THE NEXT GENERATION (FIPS 140-2)

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

*Panel Members:* Ray Snouffer, NIST
Tom Casar, Communications Security Establishment (CSE) of the Government of Canada

*Session Abstract*: The Cryptographic Module Validation Program was initiated in 1994. Cryptographic modules are tested against requirements documented in FIPS 140-1, *Security Requirements for Cryptographic Modules.* Security requirements cover 11 areas related to the design and implementation of a cryptographic module. The standard identifies requirements for four security levels for cryptographic modules to provide for a wide spectrum of data and a diversity of application environments. By February 1999, over 40 modules had been validated covering all four security levels specified in the standard.

Since the beginning of the program, NIST and the Communications Security Establishment (CSE) of the Government of Canada have issued *Implementation Guidance,* policy, and interpretations to assist the commercial laboratories in performing their validations of modules against the standard. In the fall of 1998, NIST published a Federal Register Notice announcing the five-year review of FIPS 140-1, to consider new or revised requirements that may be needed to meet technological and economic changes. The guidance issued by NIST and CSE, and public comments submitted in response to the Federal Register announcement are being evaluated for technical impact and incorporation into the revised standard (FIPS 140-2).

The panel will provide information on the revised standard plus a summary of cryptographic modules that have been validated to date. Specific topics include:

*Ray Snouffer,* NIST, will discuss the overwhelming success and positive impact of the Cryptographic Module Validation Program (CMVP), provide an overview of the CMVP, a summary of modules validated, and program status.

*Tom Casar,* CSE, will discuss the impact of the revised standard in Canada and describe the importance of the CMVP to the Canadian product endorsement program.

*Annabelle Lee*, NIST, will discuss the FIPS 140-2 revision process, discuss the current status of FIPS 140-2, and summarize the submitted comments and changes to the standard and the Derived Test Requirements (DTRs).

*Points of Contact:* Annabelle Lee, NIST (primary point of contact)
301.975.2941 (phone)
301.948.1233 (fax)
annabelle.lee@nist.gov

Ray Snouffer, NIST
301.975.4436 (phone)
301.948.1233 (fax)
ray.snouffer@nist.gov

Tom Casar, CSE
613.991.7202 (phone)
613.9917251 (fax)
tjcasar@its.cse.dnd.ca

*Biographies:*

**Annabelle Lee**

Annabelle has worked as a Systems Engineer/Computer Specialist for over twenty years. She began her career in private industry concentrating on software testing and quality assurance. After ten years in private industry she worked for The Mitre Corp. in systems engineering and information security. Ms. Lee developed and implemented an information security program for the Criminal Justice Information Services (CJIS) Division at the FBI. She also coordinated the certification and accreditation effort for a DEA program. Ms. Lee began her career in the Federal Government as the National Program Manager for Key Escrow at the National Institute of Standards and Technology (NIST) in the fall of 1996. She currently supports the FIPS 140-1 Cryptographic Module Validation Program, has developed a Guideline for Implementing Cryptography in the Federal Government, and is the technical lead for the development of FIPS 140-2.

**Ray Snouffer:**

Mr. Snouffer has worked as a mathematician for the U.S. Federal Government since October of 1987. He began his career with the Defense Information Systems Agency (DISA) serving in a variety of roles including senior mathematician, lead software developer, and Project Officer for the Strategic Defense Analysis Project. In June of 1994, Mr. Snouffer accepted the position of Deputy National Program Manager for the

U.S. Government=s Key Escrow program at the National Institute of Standards and Technology (NIST); taking over the position of National Program Manager in November of 1995. Since January 1997, Mr. Snouffer has served as the Program Manager for the Cryptographic Module Validation Program and now also serves as the supervisor of the Cryptographic Security Testing Program Area of NIST's Computer Security Division.

**Tom Casar:**

Mr. Tom Casar is employed by the Communications Security Establishment as a Cryptographic Systems Evaluation Engineer, testing and evaluating cryptographic products for use by the Government of Canada. He is the Canadian certifying technical authority for the joint NIST/CSE Cryptomodule Validation program, and also participates in the drafting of standards in the security and cryptography field.

*Audience:* This presentation is intended for government agencies, companies wishing to implement tested and validated products, and vendors interested in producing FIPS 140-1/2 compliant modules.