Title of Panel: The Cryptographic Module Validation Program: FIPS 140-2 …The Next Generation

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 and Panel Position Statements:

Federal agencies, industry, and the public now rely on cryptography to protect information and communications used in critical infrastructures, electronic commerce, and other application areas. Cryptographic modules are implemented in these products and systems to provide cryptographic services such as confidentiality, integrity, non-repudiation and identification and authentication. Adequate testing and validation of the cryptographic module against established standards is essential for security assurance. Both Federal agencies and the public benefit from the use of tested and validated products. Without adequate testing, weaknesses such as poor design, weak algorithms, or incorrect implementation of the cryptographic module can result in insecure products.

On July 17, 1995, NIST established the Cryptographic Module Validation Program (CMVP) that validates cryptographic modules to Federal Information Processing Standard FIPS 140-1 (Security Requirements for Cryptographic Modules), and other FIPS cryptography based standards. The CMVP is a joint effort between NIST and the Communications Security Establishment (CSE) of the Government of Canada. Products validated as conforming to FIPS 140-1 are accepted by the Federal agencies of both countries for the protection of sensitive information. Vendors of cryptographic modules use independent, accredited testing laboratories to test their modules. NIST's Computer Security Division and CSE jointly serve as the validation authorities for the program, validating the test results. As of August 2000 over 100 cryptographic modules from more than forty separate vendors have been validated through the program. The number of validated modules has nearly doubled each year of the program's existence.

From the beginning, the CMVP has been dynamic with a constant reexamination of the underlying standard, test methodology, reporting structure, and associated documentation. In addition, questions from the vendor and user communities have provided valuable input and an implementation perspective. NIST and CSE have continually kept pace with new security methods, changes in technology, and required interpretations of the standard by issuing official Implementation Guidance and Policy for FIPS 140-1 and associated Derived Test Requirements. The Implementation Guidance covers program policy, technical questions, and general guidance needed for module validation.

In addition to constant reexamination, the standard is officially reexamined and reaffirmed every five years. In the Fall of 1998, FIPS 140-1 entered a regularly scheduled 5-year review to consider new and/or revised requirements needed to meet technological and economic change. A request for comments on FIPS 140-1 was published on October 23, 1998 in the Federal Register. The official comment period for the request closed January 21, 1999. A revised draft standard was produced based on the public comments received, previously issued implementation guidance and a "line by line" review by the NIST, CSE, and testing laboratory staff. A second request for comments on the resulting FIPS 140-2 draft was published on November 17 in the Federal Register with a closing date of February 15, 2000. Completion of the FIPS 140-1 update to FIPS 140-2 is anticipated by October 2000.

The panelists will provide detailed information on the revised standard, including a detailed description of the revisions and impact to Federal agencies, users, and vendors. Additional 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, and program status and the schedule for implementing the new standard.

Tom Casar, CSE, will discuss the submitted comments that are reflected in revisions to FIPS 140-2, the impact of the revised standard in Canada and describe the importance of the CMVP to the Canadian product endorsement program.

Points of Contact Information and Biographies:

Annabelle Lee, NIST
301.975.2941 (phone)
301.948.1233 (fax)
annabelle.lee@nist.gov

Ms. Lee has over 25 years experience in Information Systems. Prior to working at NIST, Ms. Lee worked for the Mitre Corporation as a Lead Engineer in the Criminal Justice and Public Safety Division. She provided support to the Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Division and the El Paso Intelligence Center (EPIC) Information System (EIS) for the Drug Enforcement Administration. She was also author and co-author of documents in the "rainbow" series, the security standard for the federal Government. Currently, Ms. Lee is a Computer Specialist in the Information Technology Laboratory, Computer Security Division. Ms. Lee supports the Cryptographic Module Validation Program (CMVP) serving as the primary point of contact for three of the four testing laboratories. She also is the technical lead for the update of FIPS 140-1, *Security Requirements for Cryptographic Modules*. In addition, Ms. Lee recently authored the *Guideline for Implementing Cryptography in the Federal Government.*

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

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, CSE
613.991.8121 (phone)
613.9917251 (fax)
tjcasar@its.cse.dnd.ca

Tom Casar graduated in 1991 from McGill University with a Bachelor's degree in Computer Engineering and a Minor in Management. After three years of employment as a PC designer and a hardware designer of radio modems, Tom joined the

Communications Security Establishment in 1994 as an IT Security Engineer. Tom's duties have ranged from the testing and evaluation of high-grade and commercial cryptographic products, to the writing of cryptographic guidance and standards. He has been involved as the Canadian Technical Program Manager for the CMVP since its inception, participating in the daily management of the program, and well as in the analysis of test reports and other technical duties. Tom is also a member of the Professional Engineers of Ontario, and is an avid breeder of very large and very rambunctious German Shepherds.