CMVP Symposium BIOGRAPHIES

(In order of appearance)

Jean Campbell

Mr. Campbell is the Cryptographic Module Validation Program (CMVP) Technical Authority for the Government of Canada working as an IT Security (COMSEC) Engineer in the Cryptographic Security Section of the Communications Security Establishment (CSE). Jean joined the CSE in 1999 and he has been employed in various management functions including Designated Cryptographic Systems Program Manager and Senior Client Services Consultant. Prior to coming to the CSE, Jean retired from the Canadian Forces after a successful 20-year career in the Communication and Electronics Branch. As an officer, he was the head of various IT management sections responsible for, among other things, IT security and COMSEC issues. Jean graduated from the Royal Military College of Canada, Kingston in May of 1991 with a Bachelor of Engineering (Electrical).

Randall J. Easter

Mr. Easter is the Director and lead technical engineer of the National Institute of Standards and Technology (NIST) Cryptographic Module Validation Program (CMVP). Mr. Easter graduated in 1978 from the Pennsylvania State University with a Bachelor's degree in Electrical Engineering. Prior to joining NIST, Mr. Easter worked for the IBM Corporation in Poughkeepsie, NY. He was Senior Engineer for cryptographic hardware development; having designed and developed the first validated FIPS 140-1 Level 4 single chip cryptographic coprocessor, the S/390 CMOS Cryptographic Coprocessor. He is the author of twelve filed patents. He joined NIST's Computer Security Division in 2000. Duties include the testing and validation of high-grade commercial cryptographic modules, ISO 9000:2000 certified lead auditor, Cryptographic Module Testing (CMT) Laboratory auditor, editor of FIPS Pub 140-2, FIPS 140-2 Derived Test Requirements (DTR), FIPS 140-2 Implementation Guidance (IG), and CMVP FAQ's, editor of the ISO/IEC 19790 Information technology – Security techniques – Security requirements for cryptographic modules, and the writing of other cryptographic guidance and standards and CMVP web site maintenance.

Miles E. Smid

Mr. Smid is the Vice President for Information Assurance at Orion Security Systems. In this role he consults on a variety of security matters including cryptography, cryptographic key management, key establishment and the NIST Cryptographic Module Validation Program. Previously Mr. Smid was the Director of the CygnaCom Cryptographic Equipment Assessment Laboratory, which tests products for conformance to U.S. Government cryptographic standards. In addition, as an employee of NIST, he was responsible for the development of Security Requirements for Cryptographic Modules (FIPS 140-1) and the Advanced Encryption Standard (FIPS 197) programs.

Edward Roback

Mr. Roback serves as Chief of the Computer Security Division (CSD) at the National Institute of Standards and Technology (NIST) supporting the agency's responsibilities to protect sensitive Federal information and promote security in commercial information technology products. NIST-CSD also leads the implementation of NIST's responsibilities under the Federal Information Security Management Act of 2002 and the Cyber Security Research and Development Act of 2002. These efforts include work in the area of security standards, testing, e-authentication, studying security issues with emerging technologies, and developing security guidelines for Federal agencies. Mr. Roback heads NIST's participation on the NIST/NSA Technical Working Group and serves on the Committee on National Security Systems. He chaired NIST's algorithm selection committee for the Advanced Encryption Standard and served as Executive Secretary of the "Computer System Security and Privacy Advisory Board." He has also served on the U.S. Inter-agency Working Group on Cryptography and the U.S. delegation to the OECD Ad hoc Group of Experts on Cryptography Policy. He has chaired the Federal Agency Computer Security Programs Managers' Forum and co-authored An Introduction to Computer Security: The NIST Handbook. He recently authored NIST's Guidelines to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products.

Prior to joining NIST in 1989, he worked at the U.S. Department of State's Office of Information Systems Security. As a Presidential Management Intern at the Department, he concentrated on the development of systems security policy for the Department's classified and unclassified systems. He participated in the computer security evaluation program, leading teams to evaluate computer security of classified and unclassified systems at U.S. Foreign Service missions worldwide. Mr. Roback received his M.A. at the University of Illinois at Urbana-Champaign in Political Science and holds a B.S. in Mathematical Economics and Computer Science from Rose-Hulman Institute of Technology.

Ken Lu

Mr. Lu possesses a Bachelor degree in Electrical Engineering and a Master degree in Computer Science. He is a member of the Professional Engineers of Ontario. He had 11 years working experience in private industry including aerospace, telecommunication, automobile, banking industries. He worked in the physical security field at the Royal Canadian Mounted Police for six years. He has been working in the COMPUSEC and COMSEC fields at Communications Security Establishment since 1989. He successfully lead an evaluation team to complete the first FIPS 140-1 cryptographic module and smoothly transferred the cryptographic module testing responsibility to an accredited test laboratory located in Ottawa, Ontario, Canada.

Sharon Keller

Ms. Keller has worked as a computer scientist for the U.S. Federal Government since October of 1983. She joined NIST's Computer Security Division in 1988. Ms. Keller is the Director of the NIST Cryptographic Algorithm Validation Program. She has designed and developed cryptographic algorithm validation systems for various cryptographic algorithms including DES, Triple DES (TDES), and RSA. Other duties include validating algorithm implementations and writing guidance. Ms. Keller received a Master's Degree in Information and Computer Science and a Bachelor of Arts degree in Computer and Information Sciences and Mathematics (double major). Both degrees were obtained from Hood College, Frederick, Maryland.

Jeffrey Horlick

Mr. Horlick, a physicist, is the Technical Advisor for the National Voluntary Laboratory Accreditation Program (NVLAP) at the National Institute of Standards and Technology. He is the Program Manager for the NVLAP Cryptographic Module Testing Laboratory Accreditation Program. His areas of laboratory accreditation specialty are quality systems, information technology security testing, electromagnetic compatibility and telecommunications, and laboratory proficiency testing. Mr. Horlick is the NVLAP representative to several international organizations and he participated in the creation of several international Mutual Recognition Arrangements. Mr. Horlick has been at NIST since 1967 and has been with NVLAP since 1979.

Ghislain Lagacé

Mr. Lagacé is the Industry Program Manager working in the Cryptographic Security Section of the Communications Security Establishment (CSE). Ghislain joined CSE in August 2001. As the Designated Cryptographic Systems Program Manager, he manages the CMVP, the Cryptographic Endorsement Program and the ITS Product Pre-qualification Program. The latter two programs are aimed strictly for the Government of Canada. Prior to coming to CSE, Ghislain retired from the Canadian Forces after a successful 35-year career in the Communication and Electronics Branch. As an officer, he was the head of various IT management sections responsible for, among other things, IT security and COMSEC issues.

Dave Bettinger

Mr. Bettinger has 13 years experience in the development of satellite networking equipment, and has led the development activities and served as lead architect at iDirect Technologies since 1996. Previously, he was a senior member of the technical staff at Hughes Network Systems in the Satellite Networks Division

where he developed two generations of the flagship satellite product line, the Personal Earth Station (PES). Mr. Bettinger is a graduate of Virginia Tech with a Bachelor and Master of Science in Electrical Engineering.

Ray Potter

Mr. Potter is the manager of the Security Certifications and Assurance Program at Cisco Systems, Inc. He is responsible for the direction, strategy, and operations of Cisco's global security certification and assurance initiatives, including the FIPS 140, Common Criteria, and ICSA programs. He is the single point of contact for standards bodies, Cisco's customers, and Cisco's product teams. He has presented in several public forums on the subject of certification/assurance, including the ICSA Consortia, the Information Assurance Task Force, and the International Common Criteria Conference. Ray has also been a guest lecturer at James Madison University. Prior to working at Cisco Systems, Ray was a security engineer at a small security certification consulting company, where he helped a variety of vendors meet FIPS 140-1 and FIPS 140-2. He was also a consultant with a global management-consulting firm, assisting two Fortune 500 companies and one large government agency implement IT solutions and process improvement initiatives.

Kathy Kriese

Ms. Kriese is a Senior Product Manager at RSA Security, Inc. in San Mateo, CA. Ms. Kriese is responsible for the product direction and business development of the RSA BSAFE line of cryptography, certificate management, secure sockets layer (SSL) transport, and Web Services Security products. Ms. Kriese also manages RSA Security's participation in the National Institute for Standards in Technology (NIST) process for cryptography solution validation known as FIPS 140. For the past 12 years, Ms. Kriese has been using her marketing skills to grow the business of consumer product and high-tech companies.

Marcus Streets

Mr. Streets is the Security Standards Officer at nCipher Corporation Ltd. He is responsible for ensuring that all of nCipher's products meet the relevant security standards. For most of nCipher's customers this is FIPS 140-2. nCipher has a policy of continued product improvement. Each new product requires recertification. This policy means nCipher has more FIPS 140-1 and FIPS 140-2 certificates than any other vendor. Marcus has worked on all of nCipher's 47 validations, the 10 products currently in prevalidation and on those in development. nCipher continue to introduce new and innovative products, often introducing solutions that require careful explanation to NIST/CSE. Marcus will therefore be involved with FIPS 140-2 and FIPS 140-3 validations for many years to come.

Ray Snouffer

Mr. Snouffer has worked as a mathematician for the U.S. Federal Government since 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 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 1995. From 1997 to 2001, Mr. Snouffer served as the Program Manager for the Cryptographic Module Validation Program (CMVP). In this position he personally oversaw the validation of over 180 cryptographic modules, including the first level 2 software module, the first internet browser, the first level 3 module and level 4 module. Mr. Snouffer also wrote two of the eleven sections of FIPS 140-2 – *Mitigation of Other Attacks* and *Self-test* and is the designer and developer of the CRYPTIK tool used by the CMVP laboratories to record and analyze test results. He now manages the Security Testing and Metrics Group of NIST's Computer Security Division, which houses the CMVP.

Ron Ross

Dr. Ross is a senior computer scientist and information security researcher at the National Institute of Standards and Technology (NIST). He currently leads the FISMA Implementation Project, which includes the development of key security standards and guidelines for the Federal government and critical information infrastructure. A 1973 graduate of the United States Military Academy at West Point, Dr. Ross served in a variety of leadership and technical positions during his twenty-year career in the United States Army. During his military career, Dr. Ross also served as a White House aide and as a senior technical advisor to the Department of the Army. Dr. Ross holds both Masters and Ph.D. degrees in Computer Science from the United States Naval Postgraduate School.

Edward Morris

Mr. Morris, Director of Atlan Laboratories, has been involved with the FIPS program since 1998, and after co-founding Atlan in 2000, Mr. Morris helped develop Atlan from its very first validation into becoming the leading laboratory of FIPS 140-2 product validations. Mr. Morris has extensive experience with many different types of developing technologies ranging from network devices to software products to token devices and has used this knowledge to extend the breadth of Atlan's experience and expertise. Mr. Morris continues to provide technical expertise while focusing on improving Atlan's customer service.

Stan Kladko

Mr. Kladko, is the Director of BKP Security Labs. He previously held research positions at the Javasoft Division of Sun Microsystems, at Stanford University and at the Theoretical Division of Los Alamos National Laboratory, New Mexico, where he was named Director's Fellow. Stan is an author of more than 20 scientific publications, and was an invited speaker at a number of meetings, including JavaOne conferences and European Conference on Security and Counterterrorism. He holds Ph.D. Summa Cum Laude in Theoretical Physics from Max Planck Institute, Germany. For his research he was awarded 1998 Otto Hahn Medal of Max Planck Society.

Daun-Marie Curts

Ms. Curts, CEAL Director, has been a member of CEAL since December 2000 where she has participated in over 40 validations. She provides consulting and training to customers worldwide. She coordinates with Common Criteria Laboratories for products undergoing CC and FIPS testing. She has earned a B.S. in Computer Science from GMU and a Post-graduate Certificate in Information Security from GWU and continues to work on her M.S. in Engineering Management at GWU. She has experience with CC, HIPAA, IBIP, IPMAR, and ESRA standards. Ms. Curts is also a substitute professor for the Computer Science Department at GMU.

Dawn Adams

Ms. Adams has BSc in Mathematics and is currently the Lab Manager of the COACT Inc. CAFE Lab in Columbia, Maryland. She began her FIPS career as a member of one of the three original FIPS labs accredited by NVLAP. She has also developed documentation for FIPS validations while working for a consulting firm. She has developed a mapping between the FIPS 140-1 and FIPS 140-2 and the Common Criteria standards for CSE that was used as input to develop the Canadian CC cryptographic policy.

Greg Scorsone

Mr. Scorsone joined the DOMUS IT Security Laboratory in May 1996 and has over ten years IT security experience. Mr. Scorsone is currently the Director and leads the DOMUS FIPS evaluation team, which to date is responsible for the validation of more than 150 cryptographic modules. Mr. Scorsone earned an MBA from the University of Ottawa, is a CISSP, and is accredited as a Common Criteria EAL 4 evaluator.

Erin Connor

Mr. Connor is the Manager of Information Technology Security Evaluation & Testing at Electronic Warfare Associates - Canada, a company that specializes in IT Security Engineering Services. Erin's main responsibility is to oversee the operations of EWA-Canada's nationally accredited IT security laboratory. The lab carries out conformance testing of cryptographic products to FIPS 140-2 (Security Requirements for Cryptographic Modules) and related standards; conducts evaluations of general IT security products to ISO 15408 (Common Criteria for IT Security Evaluation); and certifies devices for connection to the *Interac*® financial services networks. Erin previously enjoyed a successful 20-year career as an engineer in the Canadian Navy.

Travis Spann

Travis Spann is a Security Engineer and FIPS 140-2 Business Area Lead at InfoGard. Mr. Spann joined InfoGard Laboratories in 2002 as a Security Engineer after obtaining his BS in Management Information Systems. At InfoGard, Mr. Spann's responsibilities include managing the FIPS 140-2 area of business as well as performing FIPS 140-2 validation testing. He oversees the FIPS 140-2 projects at InfoGard. Mr. Spann is the primary FIPS 140-2 trainer for InfoGard employees and customers around the world. Mr. Spann has been instrumental in streamlining the FIPS 140-2 process at InfoGard and enhancing customer satisfaction.

Hugh Griffin

Mr. Griffin is the Laboratory Director for the LogicaCMG FIPS Lab. Along with three others, he set up the first UK lab in 2002 and has performed the FIPS testing for two software modules (Certificates #307 and #447). Hugh joined the Logica CLEF in 1995 and has successfully managed 12 diverse ITSEC and Common Criteria (CC) evaluations: network products to operating systems to composite Military systems. This experience led him into training recruits in CC, advising clients on test strategies and introducing clients to the technical and programmatic aspects of security evaluations.