6th Annual IT Security Automation Conference

September 27-29, 2010 • Baltimore, Maryland
Baltimore Convention Center

Conference Agenda

Monday, September 27

7:00 – 9:00 am	**Registration and Breakfast** – Foyer				
8:30 – 10:15 am	**General Session** – Ballroom I **Welcome Address** **Keynote Address: Honorable Howard A. Schmidt, White House Cybersecurity Coordinator** **Keynote Address: Phil Reitinger, Deputy Undersecretary, DHS** **Track Lead Address**				
10:15 – 10:45 am	**Break** – Vendor Expo Hall				
	AUTOMATION SPECIFICATIONS	**FDCC/USGCB**	**SOFTWARE ASSURANCE**	**SCAP 101 TUTORIAL**	**AUTOMATION CONTENT TUTORIAL**
	Ballroom II	Room 316/317	Room 318/319	Ballroom I	Room 321-323
10:45 – 11:30 am	**Automation Specifications Overview** – Paul Cichonski, BAH	**Evolution of the USGCB** – William Corrington, Dept. of the Interior	**SwA Panel: Use Cases, Standards and Roadmap for Enterprise Security Automation** – Joe Jarzombek, DHS, Don Davidson, DoD, Dan Schmidt, NSA, Tim Grance, NIST, Bob Martin, MITRE	**SCAP Overview (NIST 800-126 & 800-117) –** Karen Scarfone, G2	**Innovation within SCAP Content Streams** – Kent Landfield, McAfee
11:45 – 12:30 pm	**Enterprise Remediation Automation** – Chris Johnson, NIST	**Overcoming Technical Challenges in the Windows Baselines –** Kurt Dillard, G2	**Knowing Your Weaknesses: CWE™** – Bob Martin, MITRE	**XCCDF Tutorial** – Bryan Worrell, MITRE	**Easily Create SCAP Content Using the MACE Wizard** – Tina Ackerman, NSA
12:30 – 1:30 pm	**Lunch** – Vendor Expo Hall				
1:30 – 2:15 pm	**CEE** – William Heinbockel, MITRE	**Lessons Learned from Our FDCC Customers: Unmanaged to Managed** – Shelly Bird, Microsoft	**Ranking Your Weaknesses: CWSS™** – Steve Christey, MITRE	**OVAL® Tutorial** – Matt Hansbury, MITRE	**Verification of SCAP Content** – Harold Booth, NIST
2:30 – 3:15 pm	**The Use of Rules in EMAP** – George Saylor, G2	**Moving Baselines Forward** – Kent Landfield, McAfee	**Understanding How They Attack Your Weaknesses: CAPEC™** – Sean Barnum, MITRE	**Standards Toolkit** – Dave Mann, MITRE	**The MITRE Recommendation Tracker (RT)** – Bryan Worrell, MITRE

3:15 – 3:45 pm	**Break** – Vendor Expo Hall				
3:45 – 4:30 pm	**ARF** – John Wunder, MITRE and Adam Halbardier, BAH	**Lessons Learned Using SCAP Tools** – Scott Armstrong, Symantec, Tony Uceda-Velez, Symantec	**Sharing Understanding of Malware: MAEC™** – Penny Chase, MITRE	**CCE™ & CPE™ Tutorials** – Dave Mann, MITRE	**SCAP Content Creation Solutions Using the eSCAPe Editor and Libraries** – Peter Parker, G2
4:45 – 5:30 pm	**Vendor Interoperability Panel** – Tim Keanini, nCircle (moderator), Luis Nuñez, Cisco, Kent Landfield, McAfee, John Bordwine, Symantec, Jeff Spitulnik, IBM, Todd Dolinsky, HP	**Understanding the Red Hat Enterprise Linux Baseline Settings** – Steve Grubb, Red Hat	**SwA Panel on a Software Assurance Automation Protocol (SwAAP)** – Steve Quinn, NIST, Joe Jarzombek, DHS, Dan Schmidt, NSA	**CVE® & CVSS** – Steve Christey, MITRE	**Secure Configuration Management: DoD Use Cases for SCAP and Securing Configurations** – Jim Shelton/Mike Kinney, NSA, Dave Hoon, DISA
5:30 – 7:00 pm	**Reception –** Vendor Expo Hall and Foyer				

Tuesday, September 28

7:30 – 8:30 am	**Registration and Breakfast** – Foyer				
8:30 – 10:15 am	**General Session** – Ballroom I **NIST Address: Tim Grance, Program Manager, Cyber & Network Security Program, NIST** **NSA Address: Tony Sager, Chief of the Vulnerability Analysis and Operations Group, NSA** **Keynote Address: Stephen Pawlowski, Senior Fellow and CTO for the Intel Architecture Group, Intel Corporation** **Track Lead Address**				
10:15 – 10:45 am	**Break** – Vendor Expo Hall				
	AUTOMATION SPECIFICATIONS	**NETWORK AUTOMATION**	**INNOVATIVE USES OF SCAP**	**SECURITY MANAGEMENT AND COMPLIANCE AUTOMATION**	**SECURITY AUTOMATION FOR CLOUD COMPUTING**
	Ballroom II	Room 316/317	Ballroom I	Room 318/219	Room 321-323
10:45 – 11:30 am	**XCCDF** – Charles Schmidt, MITRE	**Extending SCAP into the VMware virtual infrastructure** – Robert Hollis, ThreatGuard, Chris Farrow, VMWare	**SCM 2007 Microsoft** – Michael Tan, Microsoft	**IT Security: Tying the Pieces Together** – Mischel Kwon, RSA	**Cloud Security Opening Address** – Peter Mell, NIST, Dennis Moreau, RSA
11:45 – 12:30 pm	**CPE™** – Brant Cheikes, MITRE	**SCAP in Cloud Computing (continued)** – Robert Hollis and Randal Taylor, ThreatGuard, Chris Farrow, VMWare	**ISA VoIP Security Project** – Tom Grill, VeriSign, Paul Sand, Salare Security	**Introduction to CyberScope –** Alfredo Rohweder	**Security Automation in Private Clouds Panel** – Neil Ziring, NSA (moderator), Mischel Kwon, RSA, Steve Orrin, Intel, Jen Nowell, Symantec, Gregg Brown, Microsoft

Tuesday, September 28

12:30 – 1:30 pm	**Lunch** – Vendor Expo Hall				
1:30 – 2:15 pm	**OVAL®** – Jon Baker, MITRE	**Automated Network Security Assessments** – Doug Dexter, Cisco	**Threat Assessment and Continuous Risk Dashboard/Risk Scoring** – Kim Watson, NSA, Dr. George Moore, Dept. of State	**Client Technologies that Help Assist with Security and Privacy Regulation Compliance –** David Houlding, Intel Health	**Continuous Monitoring for Cloud Panel** – Peter Mell, NIST, Christopher Hoff, Cisco, Kent Landfield, McAfee. Duncan Hays, IRS
2:30 – 3:15 pm	**OCIL** – Maria Casipe, MITRE	**TNC: Open Standards for Network Security Automation** – Steve Hanna, Juniper Networks	**Automated Creation of SCAP Content** – Peter Guerra and Shane Shaffer, G2	**Continuous Monitoring Panel** – Peter Mell (moderator), COL Michael Jones, HQDA, John Streufert, Dept. of State, Tim McBride, DHS	**Creating Trustworthy Cloud Systems** – Ron Knode, CSC, Steve Orrin, Intel
3:15 – 3:45 pm	**Break** – Vendor Expo Hall				
3:45 – 4:30 pm	**National Checklist Program Submission Interface** – Charles Wergin, BAH, Harold Owen, G2	**Security Coordination with IF-MAP** – Matt Webster, Lumeta	**SCAP Compliance Checker: Developing a Government-Funded SCAP Validated Application** – Jack Vander Pol and Kyle Stone, SPAWAR	**Configuration Management** – Kelley Dempsey, NIST	**The Need for Software Security Assurance to Secure Mission Critical Applications in the Federal Cloud** – Rob Roy, Fortify
4:45 – 5:30 pm		**Progress in Near-Real Time Attack Detection at the Platform Level** – Dr. Bruce Gabrielson, Booz Allen Hamilton	**Leveraging SCAP for TNC, Endpoint Sensor Grid and Automated Remediation** – Jim Ivers, Triumfant	**FISMA Automation in a Global Enterprise** – Earnest Neal, Atlantic Systems Group, Inc., Dirk Barrineau, VA	**Standards to Acceleration to Jumpstart Adoption of Cloud Computing** – Lee Badger and Chris Johnson, NIST

Wednesday, September 29

7:30 – 9:00 am	**Registration and Coffee** – Foyer				
9:00 – 10:00am	**General Session Panel/Discussion** – Ballroom I				
10:00 – 10:30 am	**Break**				
	SCAP WORKSHOP	**EMAP WORKSHOP**	**REMEDIATION WORKSHOP**	**SCAP PRODUCT VALIDATION WORKSHOP**	**CONTINUOUS MONITORING WORKSHOP**
	Ballroom I	Room 316/317	Room 321-323	Room 318/319	Ballroom II
10:30 – 11:15 am	**XCCDF** – Charles Schmidt, MITRE	**EMAP Status Update**	**Common Remediation Enumeration (CRE)**	**Program Summary**	**Foundations for CM** – Peter Mell, NIST, Harold

Wednesday, September 29					
			and Extended Remediation Information (ERI) – Chris Johnson, NIST (moderator)		Booth, and Dave Waltermire, NIST
11:30 – 12:15 pm	**XCCDF** – Charles Schmidt, MITRE	**OEEL Engineering Session**	**Remediation Policy** – Matthew Wojcik, MITRE (moderator)	**Derived Test Requirements from the SCAP Specification**	**CM Technical Design Panel** – Peter Mell, NIST (moderator), Kim Watson, NSA, Ron Gula, Tenable, Duncan Hays, IRS, Randy Barr, Qualys
12:15 – 1:15 pm	**Lunch** – On your own				
1:15 – 2:00 pm	**Vulnerability Data Model** – Harold Booth, NIST	**CERE Engineering Session**	**Remediation Policy (continued)** – Matthew Wojcik, MITRE (moderator)	**Looking Ahead**	**Identifying Continuous Monitoring Measures** – David Waltermire, NIST, Matt Coose, DHS
2:15 – 3:00 pm	**OVAL® Future Considerations** – Jon Baker, MITRE	**CERE Engineering Session (continued)**	**Remediation Tasking** – Matthew Wojcik, MITRE (moderator)	**Looking Ahead (continued)**	**Identifying Continuous Monitoring Measures (continued)** – David Waltermire, NIST, Matt Coose, DHS
3:00 – 3:30 pm	**Break**				
3:30 – 4:15 pm	**ARF** – John Wunder, MITRE, Adam Halbardier, BAH	**Emerging Topics**	**Remediation Language** – Matt Kerr, G2 (moderator)	**Open Discussion**	**Identifying Continuous Monitoring Measures (continued)** – David Waltermire, NIST, Matt Coose, DHS
4:30 – 5:15 pm	**ARF** – John Wunder, MITRE, Adam Halbardier, BAH	**Emerging Topics (continued)**	**Secstate: Integrating SCAP and Puppet for System Lockdown** – Karl MacMillan, Tresys Technology	**Open Discussion**	**Identifying Continuous Monitoring Measures (continued)** – David Waltermire, NIST, Matt Coose, DHS

6th Annual IT Security Automation Conference

September 27-29, 2010 • Baltimore, Maryland
Baltimore Convention Center

Plenary Session Speakers

Honorable Howard A. Schmidt, Special Assistant to the President, and Cybersecurity Coordinator
White House

Howard A. Schmidt has had a long distinguished career in defense, law enforcement, and corporate security spanning more than 40 years. He brings together talents in business, defense, intelligence, law enforcement, privacy, academia and international relations through his distinguished career. He currently is Special Assistant to the President and the Cybersecurity Coordinator for the federal government. In this role Mr. Schmidt is responsible for coordinating interagency cybersecurity policy development and implementation and for coordinating engagement with federal, state, local, international, and private sector cybersecurity partners. Previously, Mr. Schmidt was the President and CEO of the Information Security Forum (ISF). Before ISF, he served as Vice President and Chief Information Security Officer and Chief Security Strategist for eBay Inc. He also served as Chief Security Strategist for the US-CERT Partners Program for the Department of Homeland Security.

Phil Reitinger, Deputy Undersecretary
DHS

Philip R. Reitinger was appointed by U.S. Department of Homeland Security (DHS) Secretary Janet Napolitano to serve as the Deputy Under Secretary for the National Protection and Programs Directorate (NPPD) on March 11, 2009. In this role, Reitinger leads the Department's integrated efforts to reduce risks across physical and cyber infrastructures. He oversees the coordinated operational and policy functions of the Directorate's subcomponents, which include Cybersecurity and Communications (CS&C), Infrastructure Protection (IP), Risk Management and Analysis (RMA), and the United States Visitor and Immigrant Status Indicator Technology (US-VISIT) program. On June 1, 2009 Reitinger also became the Director of the National Cybersecurity Center (NCSC), which is charged with enhancing the security of federal networks and systems by collecting, analyzing, integrating and sharing information among interagency partners. In this role, Reitinger is responsible for coordinating situational awareness and reporting for federal cybersecurity organizations and personnel.

Tim Grance, Program Manager, Cyber & Network Security Program
National Institute of Standards and Technology

Tim Grance is a the Cyber and Network Security Program Manager in the Information Technology Laboratory at the National Institute of Standards and Technology. He leads team of researchers in the Systems and Network Security Group and is engaged in a broad research program focused on such topics as cloud computing, access control, identity management, vulnerability analysis, privacy protections, security metrics, protocol security, smart cards, and wireless/mobile device security. In addition, he is also the Program Manager for Cyber and Network Security (CNS) Program and exercises broad technical and programmatic oversight over the NIST CNS portfolio. This portfolio includes high profile projects such as the NIST Hash Competition, Cloud Computing, Security Content Automation Protocol (SCAP), Protocol Security (DNS, BGP, IPv6), Combinatorial Testing, and the National Vulnerability Database. He has extensive public and private experience in accounting, law enforcement, and computer security. He has written on diverse topics including incident handling, intrusion detection, privacy, metrics, contingency planning, forensics, and identity management. He was named in 2003 to the Fed 100 by Federal Computer Week as one of the most influential people in Information Technology for the US Government. He is also is a recipient of the highest award from the US Department of Commerce - a Gold Medal, from the Secretary of Commerce.

Tony Sager, Chief of the Vulnerability Analysis and Operations Group
National Security Agency

Tony Sager is the Chief of the Vulnerability Analysis and Operations (VAO) Group within the Information Assurance Directorate at the National Security Agency. VAO's mission is to identify and analyze the vulnerability of information, technology, and operations for NSA customers and to actively help the national security community through guidance and standards. VAO has received recognition from private sector sources, including SC Magazine, Government Executive Magazine and SANS Institute. During his 30 year NSA career, Tony has held technical and managerial positions in Computer/Network Security and software analysis. He holds a BA in Mathematics from Western Maryland College and an MS in Computer Science from Johns Hopkins University. Tony is a civilian graduate of the US Army Signal Officer Basic Course and the National Security Leadership Course.

Stephen Pawlowski, Senior Fellow and CTO for the Intel Architecture Group
Intel Corporation

Stephen S. Pawlowski is an Intel Senior Fellow, chief technology officer for the Intel Architecture Group, and general manager for Central Architecture and Planning for Intel Corporation. He is responsible for ensuring architectural consistency across all Intel® Architecture and implementation of initiatives such as security and manageability across Intel® Core™ and Atom™ product lines. Pawlowski joined Intel in 1982. He led the design of the first Multibus I Single Board Computer based on the 386 processor. He was a lead architect and designer for Intel's early desktop PC and high performance server products and was the co-architect for Intel's first P6 based server chipsets. He helped define the system bus interfaces for Intel's P6 family processors, the Pentium® 4 processor and Itanium™ processor. He also created and led the research for Intel's agile radio architecture for a future generation of wireless products, he was the director of Corporate Technology Group's Microprocessor Technology Lab and prior to his current assignment he was the CTO of the Intel Architecture Group and General Manager of the DEG Architecture and Planning. Pawlowski graduated from the Oregon Institute of Technology in 1982 with bachelor's degrees in electrical engineering technology and computer systems engineering technology, and received a master's degree in computer science and engineering from the Oregon Graduate Institute in 1993. Pawlowski holds 56 patents in the area of system, and microprocessor technologies. He has received three Intel Achievement Awards.

6th Annual IT Security Automation Conference

September 27-29, 2010 • Baltimore, Maryland
Baltimore Convention Center

Automation Specifications Track
Ballroom II

Many of the use cases relating to Continuous Monitoring and Security Automation rely on standardized languages, metrics, and enumerations that formalize how machines communicate about IT security information. The Security Automation program defines these standardized languages, metrics, and enumerations using automation specifications that provide normative guidance pertaining to these constructs. These specifications cover multiple disparate domains and are at various levels of maturity. The Automation Specifications Track will provide a detailed overview of the current efforts relating to the formal specifications within the Security Automation Program. This track will also include presentations relating to how the community is leveraging the automation specifications to increase the level of security data interoperability in operational environments.

Automation Specifications Overview – Paul Cichonski, Booz Allen Hamilton

The NIST Security Automation Program is expanding at a rapid rate. As part of this expansion, there are a number of teams working on different automation specifications pertaining to disparate domains within IT security. This presentation will provide a brief overview of the Security Automation Program, focusing on the goals of the program and a history of the automation specifications that currently exist within the program. This presentation will attempt to paint the high-level picture of the different domains within the program and the inter-relationship between these domains. Audience members should view this presentation as an introduction to the "Automation Specification" track. The presentation will provide the appropriate references to later talks within the track that will cover certain topics in greater detail.

Paul Cichonski is an Associate at Booz Allen Hamilton and supports clients at the National Institute of Standards and Technology (NIST). Mr. Cichonski supports various initiatives at NIST including the development of the National Vulnerability Database (NVD) and the National Checklist Program (NCP) web applications. Mr Cichonski is also heavily involved in the development of specifications relating to the Security Automation Program, aimed at standardizing the communication of IT security information. Mr. Cichonski has a Bachelor's Degree in Information Sciences and Technology from Pennsylvania State University.

Enterprise Remediation Automation – Christopher Johnson, NIST

In recent years, broad adoption of the Security Content Automation Protocol (SCAP) has enabled security software products to communicate software flaw and security configuration information using common formats and nomenclature. The underlying SCAP specifications allow enterprises to precisely define policy for software inventory and configuration, vulnerability status, patch levels, and related information security requirements. Further, because these are open specifications, organizations are not bound to proprietary solutions for automated assessment, but instead can select tools from a wide range of vendors. The success of SCAP in automated system assessment has fostered research related to the development of similar open specifications in support of the remediation life cycle. This presentation will describe a suite of proposed specifications that support multiple enterprise remediation use cases.

Christopher Johnson is a Computer Scientist at the National Institute of Standards and Technology (NIST) where he manages the National Vulnerability Database software flaw analysis activities, submissions to the National Checklist Program and hosting of Security Content Automation Protocol data sources. Prior to joining NIST, Mr. Johnson worked as consultant to Federal and State government agencies and the investment banking, securities and insurance industries. Mr. Johnson was a founder and principal of an information assurance practice that provided vulnerability assessment, security architecture design, code development, certification and accreditation, and security testing and evaluation services. His research interests include security automation, software flaw analysis, and security metrics.

CEE – William Heinbockel, MITRE

The goal of EMAP is to bring the successes of SCAP to the enterprise event management space. This talk provides an overview of upcoming EMAP specifications and efforts to solve event management challenges. The focus of this talk will highlight the Common Event Expression (CEE) standard being developed to standardize event records. Emphasis will be placed on the development of an event language model using examples.

Bill Heinbockel is the creator and lead for Common Event Expression (CEE) for The MITRE Corporation. After graduating RIT in 2005, Bill has worked at MITRE supporting various standards efforts (e.g., CVE® and CWE™) and helping to improve enterprise security management (ESM) throughout the US DoD. His primary interests are improving information management in constrained environments and the evaluation of enterprise risk from cyber threats.

The Use of Rules in EMAP – George Saylor, G2

This session will present the current thinking and research on the standardized expression of rules for the Event Management Automation Protocol. The goals of the program and goals for the expression of rules for correlation, filtering, and searching log records will be discussed as well as design concepts, common use cases, and potential impacts.

George Saylor is the Technical Director of Attack Analysis at G2, Inc and leads a team of innovative security engineers and developers on numerous efforts. Mr. Saylor has over 20 years of information systems and security experience in a broad range of disciplines. His core focus areas are automation and standards in the event correlation space as well as penetration and exploitation of computer systems. Mr. Saylor is a co-founder of the OpenSCAP project, and has spoken at conferences and other forums on the subjects of security automation and analysis.

ARF – John Wunder, MITRE and Adam Halbardier, BAH

The National Institute of Standards and Technology (NIST) Interagency Report (IR) 7694 - Asset Reporting Format (ARF) and NIST IR 7693 - Asset Identification specifications are emerging security automation standards. ARF defines a format for reporting on assets, while using asset identification as a mechanism to consistently identify the asset about which those reports describe. ARF, in combination with the Asset Identification specification, is being proposed for inclusion in NIST Special Publication (SP) 800-126 - Security Content Automation Protocol (SCAP) 1.2 to support reporting on the results of SCAP assessments. This seminar is focused on an overview of the purpose, scope, use-cases and data models for ARF and Asset Identification, with an emphasize on introducing the audience to these emerging specifications and their role in the larger security automation landscape.

John Wunder is a senior software systems engineer at The MITRE Corporation who has been active in the security automation community for several years, supporting SCAP content development, security interface specifications, remediation standards, and asset management. His other work at MITRE includes support to government customers performing cyber command and control and mission assurance. He received his Bachelors in Computer Science at St. John's University and his Masters in Information Assurance at Northeastern University.

Adam Halbardier is a security professional and software engineer working for Booz Allen Hamilton. He supports the National Institute of Standards and Technology (NIST) Security Automation Program. Specifically, Mr. Halbardier developed the Security Content Automation Protocol (SCAP) Schematron rules for the SCAP Content Validation Tool, and he now maintains that tool. He is also coauthor of NIST Interagency Report (IR) 7693 – Asset Identification and NIST IR 7694 – Asset Reporting Format. Mr. Halbardier has a Bachelor's Degree in Computer and Electrical Engineering from the University of California, Irvine.

Vendor Interoperability Panel – Tim Keanini, nCircle (moderator), Luis Nuñez, Cisco, Kent Landfield, McAfee, John Bordwine, Symantec, Jeff Spitulnik, IBM, Todd Dolinsky, HP

This panel consists of a set of security vendors who would like to share their perspectives and experience as it relates to standards-based multi-vendor interoperability. These vendors will share lessons learned, unforeseen benefits, unforeseen challenges, and what it is really like to be a product vendor supporting the Security Automation Program specifications. The panel discussion will be moderated by the Chief Technology Officer for nCircle - Tim "TK" Keanini – and the panel consists of vendors such as IBM, HP, Cisco, Symantec and McAfee.

Tim Keanini's 19 years of technical expertise in the information security and gaming industries provides him with a unique perspective of customer challenges. As nCircle's CTO, Tim drives innovation and product strategy for the company. He is an active participant at the board and working group levels of several IT standards, some of them from their inception, and is driving for a day when consumers can have seamless automation across all of their vendor's products.

Luis K. Nunez is an Information Assurance Engineer with the Global Government Solutions Group within Cisco Systems based out RTP North Carolina. For the last 4 years Luis has represented Cisco in the area of Information Assurance in the US Federal sector. Luis is familiar with the IA process and is intimately familiar with DISA STIGs. Luis' expertise stems from his military experience and along with his civilian work with security consulting firms. Luis is also a board member of OVAL®.

Kent Landfield has spent over 25 years in software development, global network operations and network security arenas. He has recently taken on the responsibility of Director of Content Strategy, Architecture and Standards in McAfee® Labs. Before this, Kent managed the global Risk and Compliance Security Research teams at McAfee. His responsibility included producing the content supplied with McAfee's remediation, policy auditing, vulnerability management and NAC products. Kent was a catalyst in getting SCAP component standards adopted as the basis for product and content integration across three different technologies within McAfee. He initiated the first large scale commercial SCAP Content development team and content production architecture in the world. His team achieved the first localization of SCAP content, delivering completely localized content in eleven languages enabling SCAP products to be sold into a true global market. Kent has been involved with the development of security standards since the POSIX working groups in the late 1980s. He has also been involved with standards development in the Internet Engineering Task Force and Trusted System Interoperability Groups. He was one of the initial CVE® Editorial Board Members and is also an OVAL® Board member, a CPE™ Core Team member and is active in the emerging standards working groups.

As the Symantec Public Sector CTO, John Bordwine currently serves as a trusted advisor, providing guidance on the development of products and solutions that meet government requirements and certifications specifically focused on the Public Sector markets. John's responsibilities also include all technical activities related to Public Sector customers, which includes federal, state, and local government agencies, and education industries.

Jeff Spitulnik, Director of Product Management at BigFix, an IBM Company, has nearly 20 years experience in product development of enterprise software, interactive learning, consumer e-commerce, and healthcare automation. Jeff has also held management roles at EMC, Leapfrog, Razorfish, and Borders Group, driving brand name products that continue to generate hundreds of millions of dollars of revenue for these firms. Spitulnik holds a B.A. in Cognitive Science from Vassar College, and M.S. and Ph.D. degrees in Technology and Learning Sciences from the University of Michigan, Ann Arbor.

Todd Dolinsky is Chief Architect of the Security and Compliance Service for HP Business Service Automation. Todd joined Hewlett-Packard in 2007 as part of the Opsware acquisition, and since 2006 has been focused on the complete lifecycle of SCAP-related products. Todd holds undergraduate degrees in Computer Science and Electrical Engineering from Duke University, and a master's degree in International Affairs from Washington University in St. Louis.

XCCDF – Charles Schmidt, MITRE

This talk will cover the current state of XCCDF. It will go through the major features of the new XCCDF 1.2 specification and show how these features can be used to enhance XCCDF content. This talk will also briefly discuss some possible directions for the future of XCCDF. The talk is intended to inform current and prospective users of XCCDF of the new and potential future capabilities of the language.

Charles Schmidt is a Lead Information Security Engineer at the MITRE Corporation. He has supported security guidance development efforts for more than 10 years covering a wide range of technologies. He has directly supported the CVE®, CCE™, OVAL®, and OCIL security automation standards and is currently the moderator of the XCCDF benchmark standard. He also led the development teams for a number of supporting applications including the Windows Investigator Tool and the Benchmark Editor. Charles holds a Bachelors degree in both Mathematics and Computer Science from Carleton College and a Masters degree in Computer Science from the University of Utah.

CPE™ – Brant Cheikes, MITRE

The Common Platform Enumeration (CPE™) is a structured naming scheme for information technology systems, platforms, and packages. Version 2.2 of the CPE™ Specification was released in March 2009, defining CPE™ in terms of a formal name format, a language for describing complex platforms, a method for checking names against a system, and a description format for binding text and tests to a name. Work on a new release (version 2.3) of the CPE™ standard began in March 2010, resulting in the preparation of a suite of specification documents. This session presents an overview of CPE™ focusing on recent developments and directions for future enhancement.

Brant Cheikes is a Principal Scientist in MITRE's Information Technology Center. Since joining MITRE in 1993, Brant has both contributed to and directed a variety of advanced research projects in topics ranging from artificial intelligence applied to education and training, decision support systems, cognitive psychology of analytic reasoning, insider threat detection, security information management, and security content automation. He joined MITRE's CPE™ Project in February 2009, and took over leadership of the effort in October 2009. He holds a BS degree in Computer Engineering from Boston University, and MS/PhD degrees in Computer and Information Science from the University of Pennsylvania.

OVAL® – Jon Baker, MITRE

The current state of the Open Vulnerability and Assessment Language (OVAL®) will be discussed. Topics will include an over view of the major changes in OVAL® Version 5.6 which will be included in SCAP 1.1 as well as the most notable changes to the OVAL® Language that will be available in Version 5.8. This session will also briefly discuss some of the future plans for OVAL®.

Jon Baker is a Lead Information Security Engineer at the MITRE Corporation. He currently leads the OVAL® team at MITRE and has spent the past seven years working with colleagues, industry, and government participants to develop open community standards for security automation. During this time Jon's various roles included leading the development of the OVAL® Interpreter and the OVAL® Repository infrastructure, collaborating with the standards community to evolve the OVAL® Language, and contributing to the CPE™, OCIL, XCCDF, and SCAP efforts. Jon holds a Bachelors degree in Psychology from Tufts University and a Masters degree in Computer Science from Boston University.

OCIL – Maria Casipe, MITRE

The current state of the Open Checklist Interactive Language (OCIL) will be discussed. Current and prospective users of OCIL will be given an over view of the language, its use cases, and the capabilities it supports. This session will also briefly discuss some plans for the future of OCIL.

Maria Casipe joined the MITRE Corporation in 2004 after completing her M.S. in Computer Science at Tufts University. She received her B.S. in Computer Science and B.S. in Mathematics at the University of Massachusetts Lowell. Currently, she is pursuing two certificate programs specializing in Information Security Management and Human-Computer Interaction at Northeastern University and UMass Lowell, respectively. Her professional interests are on information security, net-centric operations, human-computer interaction, data visualization, semantic web, quantum computation, and mathematical modeling.

National Checklist Program Submission Interface – Charles Wergin, BAH, Harold Owen, G2

This presentation will include a brief overview of the history of the National Checklist Program (NCP). This overview will outline how the NCP has evolved from a repository of prose-based security guidance, to a repository designed to store security guidance expressed using the Security Content Automation Protocol (SCAP) specifications. The presentation will then focus on new NCP features designed to facilitate the dissemination and consumption of SCAP content. Such features include the addition of NCP "tiers", which NCP uses to categorize checklists based on their ability to facilitate automation of the checklist security guidance in a standardized fashion. This presentation will conclude with an overview of new web-based and web-service based NCP submission interfaces that will allow third party checklist creators to submit their content directly to the NCP and track content progress, as it is passes through the NCP approval process.

Charles Wergin is a security professional and software analyst working for Booz Allen Hamilton, currently supporting NIST's Security Automation Program. Since joining the SA program in 2007, his responsibilities include leading efforts in vulnerability analysis, quality assurance, operational and security support for the National Vulnerability Database and the National Checklist Program and their associated websites. Prior to joining the SA program, Chuck has participated in a wide range of IT roles over the last 12+ years, including software testing, system and database integration and implementation, configuration management, digital forensics tool development and testing, and IV&V of a variety of biometric capture and analysis products.

Harold Owen is a Maryland-based software developer from G2 Inc. Harold has been supporting the NIST National Vulnerability Database (NVD) and National Checklist Program (NCP) since 2009. Harold has a BS in Computer Science from the University of Central Florida, and more than 20 years of development experience with an emphasis in Java Enterprise applications.

FDCC/USGCB Track
Room 316/317

The Federal Desktop Core Configuration (FDCC) is three years old and it continues to evolve. The original OMB mandate has expanded to include baselines for Windows 7, Internet Explorer 8, and Red Hat Enterprise Linux 5 under the United States Government Configuration Baseline (USGCB) initiative. This track will include an overview of the FDCC and USGCB as well as detailed focus on the technical issues raised and addressed by some of the configuration items within the baselines. Representatives from several vendors will also discuss their experiences deploying and supporting the baselines in production environments.

Evolution of the USGCB – William Corrington, Department of the Interior

The chair of the USGCB change control board will provide a background on the USGCB, including its evolution from the Federal Desktop Core Configuration (FDCC) and vision for the USGCB moving forward.

William Corrington has over 30 years of experience in the Information Technology industry. He has worked as a software engineer,

systems architect, project manager, management consultant and entrepreneur in the areas of operating system development, factory automation, information publishing and network security. A former Vice President with Gartner Consulting's Federal practice, he joined the Department of the Interior in 2004 as the Deputy CIO for the Bureau of Land Management (BLM). At BLM he oversaw IT operations in support of over 12,000 users. He now serves as the DOI Chief Technology Officer (CTO) with responsibility for defining DOI technology strategy and architecture and leading enterprise-wide infrastructure projects.

Overcoming Technical Challenges in the Windows Baselines – Kurt Dillard, G2

In the months since the Alpha version of the Windows 7 and Internet Explorer 8 USGCB baselines were published NIST has received a great deal of valuable feedback from across the public sector community. The settings have evolved, this session will focus on the most challenging ones and why they have, or have not, been adjusted in their most recent update.

Kurt is an independent consultant who has been supporting the Federal Desktop Core Configuration (FDCC) program for nearly three years. He has been answering technical inquiries sent to NIST's FDCC and United States Government Configuration Baselines (USGCB) mailing lists (usgcb@nist.gov), developing and maintaining Security Content Automation Protocol (SCAP) content, and assisting with the creation of other resources available on the FDCC and USGCB websites. He has collaborated on numerous security guides published by Microsoft including the "Windows Server 2008 Security Guide," "Windows 7 Security Guide," and "Security Compliance Management Toolkit." He has presented at numerous conferences including RSA, TechEd, NIST's Security Content Automation Conference, and Microsoft Federal Security Summit. Current industry certifications include CISSP, ISSAP, CISM, MCITP: EA and MCSE + Security.

Lessons Learned from Our FDCC Customers: Unmanaged to Managed – Shelly Bird, Microsoft

Microsoft has a team of over 20 consultants now who have delivered dozens of Federal Desktop Core Configuration (FDCC) and US Government Configuration Baseline (USGCB) deployments to Public Sector customers. In the course of these engagements, consultants have acquired a wealth of experience on handling the move from unmanaged to managed desktops, watched the most common errors, and worked with customers on particularly difficult application compatibility and process challenges. Shelly Bird will outline where Microsoft has seen customers succeed and fail as they drive towards achieving the economies, superior security and greater agility associated with Managed Desktops.

Shelly Bird is a Solution Architect in the Public Sector Services CTO organization who focuses upon technologies that enable mass deployments of desktops and servers, particularly in areas where security is a high concern. Ms. Bird has been a Subject Matter Expert in this area for over a decade with Microsoft, leading several early efforts to standardize very large enterprises in both Civilian and Military enterprises. In 2008 she won the Circle of Excellence Platinum award from Microsoft and received recognition from Federal Computer Weekly's Fed 100, for leading a US Air Force desktop project which led directly to the Office of Management and Budget (OMB) Federal Desktop Core Configuration (FDCC) initiative. FDCC and the succeeding US Government Configuration Baseline (USGCB) have gotten a lot of recognition as an important development in government drive for standardization for security's sake; such efforts have been documented to lead to notable cost savings by Gartner and MIT CISR. Ms. Bird is now working upon efforts to widen and simplify the implementation and planning for customers who are trying to meet critical mandates for privacy and identity management.

Moving Baselines Forward – Kent Landfield, McAfee

Creating functional baselines is not an easy task. Using them can be even harder. The purpose of this talk is to describe how a vendor views working with existing content baselines and benchmark development architecture. We will discuss the goals of and issues surrounding the current baseline architecture, what pieces are missing and how we can set a foundation for dealing effectively with baselines in the future.

Kent Landfield has spent over 25 years in software development, global network operations and network security arenas. He has recently taken on the responsibility of Director of Content Strategy, Architecture and Standards in McAfee® Labs. Before this, Kent managed the global Risk and Compliance Security Research teams at McAfee. His responsibility included producing the content supplied with McAfee's remediation, policy auditing, vulnerability management and NAC products. Kent was a catalyst in getting SCAP component standards adopted as the basis for product and content integration across three different technologies within McAfee. He initiated the first large scale commercial SCAP Content development team and content production architecture in the world. His team achieved the first localization of SCAP content, delivering completely localized content in eleven languages enabling SCAP products to be sold into a true global market. Kent has been involved with the development of security standards since the POSIX working groups in the late 1980s. He has also been involved with standards development in the Internet Engineering Task Force and Trusted System Interoperability Groups. He was one of the initial CVE® Editorial Board Members and is also an OVAL® Board member, a CPE™ Core Team member and is active in the emerging standards working groups.

Lessons Learned Using SCAP Tools – Scott Armstrong, Symantec, Tony Uceda-Velez, Symantec

Utilizing the next generation discovery and assessment tools that are SCAP Validated, organizations can gain real insight into their networks, hosts, applications and measure vulnerabilities and compliance using best practices like NIST 800-53r3, FDCC or internal guidelines. This provides situational awareness and the ability to report within the organization about current threat risks, configuration compliance, vulnerability posture, and remediation actions. The rules to managing a network do not magically change with SCAP, though standardization, interoperability, and "open" non-proprietary XML content supports an approach that is often thought of as a continuous cycle, and that greatly benefits from automation. The methods used to discover, analyze, measure, remediate and report present challenges both technically and organizationally. This presentation and discussion group will address best practices and lessons learned for issues of discovery, handling rogue systems, enclave separation, results aggregation/reporting, and applying compliance rules across varying domains based upon standards-based SCAP solutions. Practitioners currently engaged with CyberScope reporting projects will find this session of significant value.

Scott Armstrong drives business development strategies and strategic partnerships for the Symantec Public Sector security team, and has a passion for industry-government alliances that help deliver next generation solutions to today's security needs. Scott has over 20 years experience delivering enterprise software & middleware & SAAS & security solutions, and has been significantly involved with the NIST SCAP (Security Content Automation Protocol) community over the last 6 years. He also and serves as a Member of the Board for the Open Vulnerability Assessment Language (OVAL®) organization managed by MITRE and funded by the US Department of Homeland Security.

An experienced security management professional, Tony Uceda-Velez has more than 15 years of hands-on security and technology experience and is a vocal advocate of security process engineering – a terminology that describes the design and development of secure processes and controls working symbiotically to a unique business workflow. Currently, Tony serves as a Principal Consultant at Symantec Corporation where his current federal work has included the deployment of Security Content Automation Protocol (SCAP) solutions across federal agencies and its underlying operating divisions. Tony's experience with SCAP encompasses the various challenges in creating, obtaining, and managing relevant and meaningful SCAP content for ongoing monitoring and measurement of federal systems.

Understanding the Red Hat Enterprise Linux Baseline Settings – Steve Grubb, Red Hat

The RHEL USGCB settings are the result of collaboration between Red Hat, NIST, NSA, DISA, and G2. This session will give an overview of the project, then focus on the threats which formed the basis for decision making, and then discuss the value and impact of some specific settings.

Steve Grubb is a Principal Engineer who leads the Security Technologies Team at Red Hat. His team works on Security Certifications and Guidance as well as maintaining many of the security tools that you find on Linux systems. One of the newest tools is the OpenSCAP project, for which he is the Project Lead. He is the primary author of the user space and some of the kernel audit code. He has been working on Linux security for over 10 years, focusing primarily on flaw discovery and repair for many of the important programs in use.

Software Assurance Track

Room 318/319

Today, automated operational security assessment is performed at the platform level through the use of SCAP-enabled tools. What type of security assessments can be performed on software before it is operational that would support automated operations? And can these assessments provide assurance insights about not just the product, but also include the process, the people, the supply chain and other factors that contribute to the operational security of an enterprise? These are the questions that will be addressed in the Software Assurance Track at ITSAC. Our track begins with a panel discussion of where we are today with respect to standards and use cases for enterprise assurance, and where we are going. We follow up with presentations on the existing knowledge collections about weaknesses, attack patterns and malware that are being used today in software assurance assessment, as well as a discussion of metrics for software weaknesses. We end the day with a panel discussion on the feasibility of a "Software Assurance Automation Protocol" (SwAAP).

SwA Panel: Use Cases, Standards and Roadmap for Enterprise Security Automation – Joe Jarzombek, DHS, Don Davidson, DoD, Dan Schmidt, NSA, Tim Grance, NIST, Bob Martin, MITRE

SCAP is the US Government's method for using open standards for automated vulnerability management, measurement, and policy compliance at the system level. An enterprise, however, consists of many other business processes, people, applications, data, infrastructure and technology that could benefit from consistent and automated measurement. This panel discusses how the future may look with respect to automation to secure the enterprise through the development of new use cases and standards beyond SCAP.

Joe Jarzombek is the Director for Software Assurance within the National Cyber Security Division of the Department of Homeland

Security. In this role he leads government interagency efforts with industry, academia, and standards organizations in addressing security needs in work force education and training, more comprehensive diagnostic capabilities, and security-enhanced development and acquisition practices. Joe served in the U.S. Air Force as a Lieutenant Colonel in program management. After retiring from the Air Force, he worked in the cyber security industry as vice president for product and process engineering. Joe also served in two software-related positions within the Office of the Secretary of Defense prior to accepting his current DHS position. He is a Project Management Professional (PMP) and a Certified Secure Software Lifecycle Professional (CSSLP). In other community volunteer activities, as an active member of Toastmasters International, Joe Jarzombek has served as International Director, and he is currently serving as Region Advisor Marketing.

Don Davidson is currently assigned to the Globalization Task Force (GTF) in OASD-NII / DoD CIO, where he leads the "outreach & standardization" effort within the Comprehensive National CyberSecurity Initiative (CNCI) task #11 on improving Supply Chain Risk Management for Information Communications Technology capabilities (ICT SCRM). He has 35 years of federal service to include 11 years active duty, as well as civilian assignments in Army Research Laboratory, Army Materiel Command, Army Secretariat, US Joint Forces Command, OSD-Acquisition, Technology & Logistics (AT&L) and now OASD-Networks and Information Integration (NII). He currently chairs a Global ICT-SCRM Ad-Hoc WG under American National Standards Institute / International Committee for Information Technology Standards (ANSI / INCITS). He serves as the government Co-Chair for the Acquisition & Outsourcing Working Group with the Software Assurance Program; SwA Program is a public-private partnership effort sponsored by DHS, DoD and DoC (NIST). He also serves as the Director for Defense Applications with the International Society of Logistics (SOLE, a 501c3 not-for-profit organization). He is a graduate of Brookings Institute's Executive Leadership 1 & 2 (2005), UNC's LOGTECH at Kenan-Flagler Business School of the University of North Carolina at Chapel Hill (2007) and the Defense Leadership and Management Program (DLAMP, 2008). He has a Bachelor of Science Degree in Engineering from USMA at West Point NY and a Master of Science Degree in National Security Strategy with concentration in Information Resources Management from the National War College (NWC) at National Defense University.

Daniel J. Schmidt is Computer Scientist serving as the Technical Director of the National Security Agency (NSA) Information Assurance Directorate (IAD) Vulnerability Analysis and Operations (VAO) Mission Integration and Technology Office. Mr. Schmidt spent 20 years as a Cryptologist while serving in the United States Navy from 1980 – 2000. Upon retirement from the United States Navy, Mr. Schmidt immediately transitioned to NSA as a federal government employee. During his time with NSA Mr. Schmidt has performed in a variety of technical leadership roles. The focus has been on the design and development of information technology based systems with a special emphasis on large scale, high volume data and information management and automation.

Tim Grance is a senior computer scientist in the Information Technology Laboratory at the National Institute of Standards and Technology in Gaithersburg, MD. He is the Program Manager for Cyber and Network Security (CNS) Program and exercises broad technical and programmatic oversight over the NIST CNS portfolio. This portfolio includes high profile projects such as the NIST Hash Competition, Cloud Computing, Security Content Automation Protocol (SCAP), Protocol Security (DNS, BGP, IPv6), Combinatorial Testing, and the National Vulnerability Database. He has extensive public and private experience in accounting, law enforcement, and computer security. He has written on diverse topics including incident handling, intrusion detection, privacy, metrics, contingency planning, forensics, and identity management. He was named in 2003 to the Fed 100 by Federal Computer Week as one of the most influential people in Information Technology for the US Government. He is also is a two time recipient of the US Department of Commerce's highest award—a Gold Medal, from the Secretary of Commerce.

Robert A. Martin is a Principal Engineer at MITRE, a company that works in partnership with the government to address issues of critical national importance. For the past 18 years, Robert's efforts focused on the interplay of risk management, cyber security, and quality assessment. The majority of this time has been spent working on the CVE®, OVAL®, CWE™, CAPEC™ and MAEC™ security standards initiatives in addition to basic quality measurement and management. Robert is a frequent speaker on the various security and quality issues surrounding information technology systems and has published numerous papers on these topics. Robert joined MITRE in 1981 with a BS and MS in EE from RPI, later he earned an MBA from Babson College. He is a member of the ACM, AFCEA, IEEE, and the IEEE Computer Society.

Knowing Your Weaknesses: CWE™ – Bob Martin, MITRE

Whether you manage internal development activities, work with third party developers or are developing a COTS application for enterprise, your mandate is clear - safeguard your code and make sure you know your weaknesses. The Common Weakness Enumeration (CWE™) initiative has created a dictionary of the common software weaknesses in architecture, design, or code for developers and security practitioners and to serve as a standard measuring stick for software security tools targeting these weaknesses, and to provide a common baseline standard for weakness identification, mitigation, and prevention efforts. The 2010 SANS/CWE™ list of the Top 25 Most Dangerous Software Errors, based on a sub-set of CWE™, is discussed by many as the "standard" of due-diligence for developing secure applications in many large enterprises, and government and industry have implement procurement contracts utilizing the list in procurement language mandating application security.

Robert A. Martin is a Principal Engineer at MITRE, a company that works in partnership with the government to address issues of critical national importance. For the past 18 years, Robert's efforts focused on the interplay of risk management, cyber security, and quality assessment. The majority of this time has been spent working on the CVE®, OVAL®, CWE™, CAPEC™ and MAEC™ security standards initiatives in addition to basic quality measurement and management. Robert is a frequent speaker on the various security and quality issues surrounding information technology systems and has published numerous papers on these topics. Robert

joined MITRE in 1981 with a BS and MS in EE from RPI, later he earned an MBA from Babson College. He is a member of the ACM, AFCEA, IEEE, and the IEEE Computer Society.

Ranking Your Weaknesses: CWSS™ – Steve Christey, MITRE

Making sure your team is working to eliminate the most important security weaknesses in your applications is a common goal whether you manage internal development activities, work with third party developers or are developing a COTS application for enterprises, To-date, each vendor and team has been left to create their own method for prioritizing these types of issues. The Common Weakness Scoring System (CWSS™) is working to create a standardized approach to this problem that would enable disparate measurements to be combined and compared so the overall weakness score for an application could be discussed and evaluated. This talk will cover the work to-date and the road ahead for this community effort within the CWE™ initiative.

Steve Christey is a Principal Information Security Engineer in the Security and Information Operations Division at The MITRE Corporation. Since 1999, he has been the Editor of the Common Vulnerabilities and Exposures (CVE®) list and the Chair of the CVE® Editorial Board. He is a technical consultant to the Common Weakness Enumeration (CWE™) project. He is a contributor to standards-based efforts such as the SANS Secure Programming exams, the Common Vulnerability Scoring System (CVSS), and others. His current interests include secure software development, vulnerability information management, post-disclosure analysis, and vulnerability research. Past work, which dates back to 1993, includes co-authoring the "Responsible Vulnerability Disclosure Process" draft in 2002, reverse engineering of malicious code, automated vulnerability analysis of source code, and vulnerability scanning and incident response. He holds a B.S. in Computer Science from Hobart College.

Understanding How They Attack Your Weaknesses: CAPEC™ – Sean Barnum, MITRE

By learning to think more like attackers, we gain a better understanding of how to defeat their methods. The Common Attack Pattern Enumeration and Classification (CAPEC™) initiative is a community-driven software security effort to create a publicly available catalog of attack patterns. At the core of CAPEC™ is the concept of an "Attack Pattern," a powerful mechanism for capturing and codifying various approaches to cyber attack including the detailed action-oriented attack execution flow, the capability and motivation of the attacker, the context within which the attack is possible, the weaknesses being targeted by the attack, characterization of the typical impact of a successful attack, and recommended mitigations to prevent or decrease the impact of the attack. This talk will serve as an overview of the CAPEC™ project to-date and showcase the various uses cases for CAPEC™ in software development, testing, architecture analysis, and secure operations.

Sean Barnum is a Software Assurance Principal at The MITRE Corporation where he acts as a thought leader and senior advisor on software assurance and cyber security topics to a wide variety of government sponsors throughout the national security, intelligence community and civil domains. He has over 24 years of experience in all of the various aspects of the software industry. He is a frequent contributor, speaker and trainer for regional and national software security and software quality publications, conferences & events. He is very active in the software assurance community and is involved in numerous knowledge standards-defining efforts including the CWE™, CAPEC™, SAFES, MAEC™ and other elements of the Software Assurance Programs of the Department of Homeland Security, Department of Defense and NIST. He is coauthor of the book “Software Security Engineering: A Guide for Project Managers”, published by Addison-Wesley. He serves as the official liaison between ISO/IEC JTC 1/SC 27/WG 3 and the Cyber-Security Naming & Information Structures Group. He also acted as the lead technical subject matter expert for design and implementation of the Air Force Application Software Assurance Center of Excellence (ASACoE).

Sharing Understanding of Malware: MAEC™ – Penny Chase, MITRE

Malware represents one of the most prevalent threats to cyber security, and is increasingly able to circumvent previously standardized detection, mitigation, and characterization techniques. Although new methods for combating malware have been developed, it is still difficult to communicate and share useful information garnered through these techniques without ambiguity and corresponding data loss. To close this significant gap, the Malware Attribute Enumeration and Characterization (MAEC™) initiative is creating a language for characterizing malware based on its behaviors, artifacts, and attack patterns. This talk will serve as an overview of the MAEC™ project as well as showcase the various uses cases for MAEC™ in malware detection, analysis, sharing, and response at both the individual system-level, network-level and as a community. MAEC™ will allow for the description and identification of malware based on distinct patterns of attributes and behaviors rather than a single metadata entity (which is the method commonly employed in signature-based detection) and sharing and collaboration across disparate malware analysis and defense efforts.

Penny Chase is a Senior Principal Scientist in the Information Technology Center at the MITRE Corporation. Penny leads the Malware Attribute Enumeration and Characterization (MAEC™) project and is co-chair of the DHS/DoD/NIST Software Assurance Forum Malware Working Group. She has led MITRE and government-sponsored projects in security visualization, software assurance, malware analysis, reverse engineering, software architecture and design pattern recovery, vulnerability scanning, legacy database encapsulation, machine learning, and constraint-based reasoning. Penny’s research has been presented at dozens of conferences. She was the Deputy Director of the ARDA Northeast Regional Research Center, managing workshops that addressed Intelligence Community challenge problems including “Indications and Warnings for Insider Threat,” “Knowledge Exploration,

Analysis, and Discovery (KNEAD)," and "IP Traceback." Penny holds a B.S. in Mathematics and History from S.U.N.Y. Binghamton, and later earned an A.M. in History of Science and an S.M. in Computer Science from Harvard University.

SwA Panel on a Software Assurance Automation Protocol (SwAAP) – Steve Quinn, NIST, Joe Jarzombek, DHS, Dan Schmidt, NSA

The Security Content Automation Protocol (SCAP) is a synthesis of interoperable open standards derived from community ideas. Together, they enable tooling for automated vulnerability management, measurement, and policy compliance evaluation. Can a similar approach to SCAP be taken with software assurance? Can existing specifications be leveraged and new specifications developed to create a US Government method for determining if security has been "built in" to software design, development and testing? Security assurance experts from NIST, DHS and NSA discuss the issues in providing the same kind of automation that SCAP provides to platform security to software assurance in general.

Stephen Quinn is a computer scientist at the National Institute of Standards and Technology (NIST). He is the co-originator of the Security Content Automation Protocol (SCAP) scap.nist.gov who also oversees the Security Automation Initiative at NIST including NIST National Checklist Program (checklists.nist.gov) and National Vulnerability Database (nvd.nist.gov). Prior to joining NIST, Steve worked as consultant to the Department of Defense and large commercial outsourcings with Wall Street banking firms and insurance companies. Specifically, he comes from an operational background, having owned a company that provided services offering for vulnerability assessments, designing security architectures, code development, C&A, and ST&Es. His research experience includes computer viruses, intrusion detection systems (IDSs), vulnerability/misconfiguration identification, categorization, and remediation

Joe Jarzombek is the Director for Software Assurance within the National Cyber Security Division of the Department of Homeland Security. In this role he leads government interagency efforts with industry, academia, and standards organizations in addressing security needs in work force education and training, more comprehensive diagnostic capabilities, and security-enhanced development and acquisition practices. Joe served in the U.S. Air Force as a Lieutenant Colonel in program management. After retiring from the Air Force, he worked in the cyber security industry as vice president for product and process engineering. Joe also served in two software-related positions within the Office of the Secretary of Defense prior to accepting his current DHS position. He is a Project Management Professional (PMP) and a Certified Secure Software Lifecycle Professional (CSSLP). In other community volunteer activities, as an active member of Toastmasters International, Joe Jarzombek has served as International Director, and he is currently serving as Region Advisor Marketing.

Daniel J. Schmidt is Computer Scientist serving as the Technical Director of the National Security Agency (NSA) Information Assurance Directorate (IAD) Vulnerability Analysis and Operations (VAO) Mission Integration and Technology Office. Mr. Schmidt spent 20 years as a Cryptologist while serving in the United States Navy from 1980 – 2000. Upon retirement from the United States Navy, Mr. Schmidt immediately transitioned to NSA as a federal government employee. During his time with NSA Mr. Schmidt has performed in a variety of technical leadership roles. The focus has been on the design and development of information technology based systems with a special emphasis on large scale, high volume data and information management and automation.

SCAP 101 Tutorial

Ballroom I

The SCAP 101 track will provide and introduction to SCAP 1.0. Participants will be given a high level overview of SCAP and each of the component standards it references.

SCAP Overview (NIST 800-126 & 800-117) – Karen Scarfone, G2

SCAP was created to provide an automated, standardized approach to maintaining the security of enterprise systems, such as implementing security configuration baselines, verifying the presence of patches, performing continuous monitoring of system security configuration settings, examining systems for signs of compromise, and having situational awareness—being able to determine the security posture of systems and the organization at any given time. An introduction to SCAP including discussion of its use cases, how to adopt SCAP in your organization, and the SCAP Validation Program will be provided.

Karen Scarfone is a Senior Security Engineer at G2, Inc., focusing on security automation technologies. She was formerly a Senior Computer Scientist for NIST, where she co-authored over 40 publications, including several of the key SCAP specification documents, and conducted extensive research into vulnerability measurement and the Common Vulnerability Scoring System (CVSS). Karen holds a B.S. in Computer Science from the University of Wisconsin-Parkside and an M.S. in Computer Science from the University of Idaho, and she is currently pursuing an M.S. in Technical Writing from Utah State University.

XCCDF Tutorial – Bryan Worrell, MITRE

The eXtensible Configuration Checklist Description Format (XCCDF) is a specification language for writing security checklists, benchmarks, and related kinds of documents. SCAP leverages XCCDF for its ability to provide a uniform foundation for expression of security checklists, benchmarks, and other configuration guidance. An introduction XCCDF will be provided including discussions of the use cases, structure of the language, and the importance of community participation in the ongoing development of XCCDF.

Bryan Worrell is an InfoSec Scientist at MITRE and has worked in the Information Security field for the last three years. Bryan currently leads the software development effort for both the Recommendation Tracker and XCCDF Interpreter. Bryan is also a member of the OVAL® Development team. Bryan attended Central Michigan University where he earned a Bachelor of Science degree in Computer Science.

OVAL® Tutorial – Matt Hansbury, MITRE

The Open Vulnerability and Assessment Language (OVAL®) an international, information security community standard to promote open and publicly available security content, and to standardize the transfer of this information across the entire spectrum of security tools and services. SCAP leverages OVAL® for low level authenticated assessment capabilities enabling the automation of end system state checking. An introduction to OVAL® will be provided including discussions of how the OVAL® Language works, use cases, structure of the language, and the importance of community participation in the ongoing development of OVAL®.

Matt Hansbury is a Lead InfoSec Scientist at MITRE, working on the OVAL® project and spending a lot of time working with the OVAL® Repository and its supporting tools. He also leads a team producing SCAP content for a government sponsor that includes XCCDF & OVAL® documents. He has a broad background in software development including government contracting, commercial websites, and health care software. Matt has a Bachelor of Science degree from Tufts University.

Standards Toolkit – Dave Mann, MITRE

A typology of different kinds of standards describing three major categories: human-oriented, machine oriented and human/machine interface standards will be discussed in the context of establishing a toolkit or set of design patterns for developing new standards and better understanding existing standards.

David Mann is a Principle Scientist at the MITRE Corporation where he primarily works on the development of cyber-security information standards. He is credited as co-founding both CVE® and CCE™. Prior to returning to MITRE in 2004, David served as a Security Product Strategist at BindView Development. He also served as a Product Manager in their Policy and Compliance group and managed their RAZOR Security Research Team. Prior to joining BindView, he worked at MITRE where he was involved in security assessment efforts and the development of several vulnerability databases and network security algorithms. He also spent several years at the Quinsoft Corporation as a programmer building database application development software and as a Visiting Professor at the Naval Postgraduate School. David holds a Ph.D. in Mathematics from Northeastern University where he worked on graph theoretic network stability metrics. David's current research interests include the sociological aspects of standards creation as they relate to data model development.

CCE™ & CPE™ Tutorials – Dave Mann, MITRE

An introduction to the Common Configuration Enumeration (CCE™) and the Common Platform Enumeration (CPE™) will be provided. CCE™ provides unique identifiers to security-related system configuration issues in order to facilitate fast and accurate correlation of configuration data across multiple information sources and tools. CPE™ is a structured naming scheme for information technology systems, platforms, and packages.

David Mann is a Principle Scientist at the MITRE Corporation where he primarily works on the development of cyber-security information standards. He is credited as co-founding both CVE® and CCE™. Prior to returning to MITRE in 2004, David served as a Security Product Strategist at BindView Development. He also served as a Product Manager in their Policy and Compliance group and managed their RAZOR Security Research Team. Prior to joining BindView, he worked at MITRE where he was involved in security assessment efforts and the development of several vulnerability databases and network security algorithms. He also spent several years at the Quinsoft Corporation as a programmer building database application development software and as a Visiting Professor at the Naval Postgraduate School. David holds a Ph.D. in Mathematics from Northeastern University where he worked on graph theoretic network stability metrics. David's current research interests include the sociological aspects of standards creation as they relate to data model development.

CVE® & CVSS – Steve Christey, MITRE

An introduction to Common Vulnerabilities and Exposures (CVE®) and the Common Vulnerability Scoring System (CVSS) will be provided. CVE® is a dictionary of common names for publicly known information security vulnerabilities. CVE®'s common identifiers—called CVE® Identifiers—make it easier to share data across separate network security databases and tools, and provide a baseline for evaluating the coverage of an organization's security tools. CVSS is a vulnerability scoring system designed to provide an open and standardized method for rating IT vulnerabilities. CVSS helps organizations prioritize and coordinate a joint response to security vulnerabilities by communicating the base, temporal and environmental properties of a vulnerability.

Steve Christey is a Principal Information Security Engineer in the Security and Information Operations Division at The MITRE Corporation. Since 1999, he has been the Editor of the Common Vulnerabilities and Exposures (CVE®) list and the Chair of the CVE® Editorial Board. He is the technical lead of the Common Weakness Enumeration (CWE™) project. He was the technical editor of the 2009 CWE™/SANS Top 25 Most Dangerous Programming Errors list and the CVE® vulnerability trends analysis, and he has been an active contributor to other efforts including NIST's Static Analysis Tool Exposition (SATE), the Common Vulnerability Scoring System (CVSS), and the SANS Secure Programming exams. Despite his active participation in community efforts, he still struggles with the definitions of apparently-simple concepts such as "vulnerability" and "risk." His current interests include secure software development and testing, understanding the strengths and limitations of automated code analysis tools, the theoretical underpinnings of vulnerabilities, making software security accessible to the general public, vulnerability information management including post-disclosure analysis, and vulnerability research. Past work, which dates back to 1993, includes co-authoring the "Responsible Vulnerability Disclosure Process" draft with Chris Wysopal in 2002, reverse engineering of malicious code, automated vulnerability analysis of source code, and vulnerability scanning and incident response. He holds a B.S. in Computer Science from Hobart College.

Automation Content Tutorial

Room 321-323

The Security Content Automation Protocol (SCAP) suite of protocols enables machine to machine exchange of critical enterprise security information. Software tools capable of leveraging SCAP content improve many functions such as automated vulnerability management, reporting, continuous monitoring, policy compliance and malware detection. These tools must have accurate SCAP content to assess the security posture of these managed systems. Generation of this content is not automated and often represents the largest barrier to SCAP adoption. This track focuses on how to generate and validate content for these tools.

Innovation within SCAP Content Streams – Kent Landfield, McAfee

There are two areas which we are expanding SCAP related uses in our products, localization and results processing. At present SCAP is considered a US-only standard. This view is invalid and sells SCAP capabilities short. McAfee has successfully produced localized SCAP content in 11 different languages today without changing the specifications of OVAL® or XCCDF. Part of the talk will describe how this is done today. SCAP can be successfully used internationally with no changes today. The second area expands the results capabilities. SCAP uses a "compliant/non-compliant" approach to results. What this means is customers are told system X or a set of systems are non-compliant. What does that mean to the administrators? It is the same situation where a user tells the software developer their software is "broke". What is broke? In this case, what was it that was discovered on the system(s) that made them appear non-compliant? McAfee has developed a capability being successfully used today known as 'Findings'. This is an extension that can be used in conjunction with XCCDF / OVAL® today to allow the user to see what the real problems were without having to dig through xml results files. Findings are being proposed as an extension standard to the community. In both cases, these are techniques fielded today that can be used to add real value to SCAP content streams without having to change the existing standards.

Kent Landfield has spent over 25 years in software development, global network operations and network security arenas. He has recently taken on the responsibility of Director of Content Strategy, Architecture and Standards in McAfee® Labs. Before this, Kent managed the global Risk and Compliance Security Research teams at McAfee. His responsibility included producing the content supplied with McAfee's remediation, policy auditing, vulnerability management and NAC products. Kent was a catalyst in getting SCAP component standards adopted as the basis for product and content integration across three different technologies within McAfee. He initiated the first large scale commercial SCAP Content development team and content production architecture in the world. His team achieved the first localization of SCAP content, delivering completely localized content in eleven languages enabling SCAP products to be sold into a true global market. Kent has been involved with the development of security standards since the POSIX working groups in the late 1980s. He has also been involved with standards development in the Internet Engineering Task Force and Trusted System Interoperability Groups. He was one of the initial CVE® Editorial Board Members and is also an OVAL® Board member, a CPE™ Core Team member and is active in the emerging standards working groups.

Easily Create SCAP Content Using the MACE Wizard – Tina Ackerman, NSA

The Malware Content Editor (MACE) is a specialized tool unique in its ability to generate Security Content Automation Protocol (SCAP) content without requiring users to fully understand XML, XCCDF, or OVAL®. The Security Content Automation Protocol (SCAP), pronounced "S-Cap", is a method of using specific standards to enable automated vulnerability management and measurement. SCAP consists of system tests written in OVAL® and enumerated in XCCDF. The content allows security operators to specify in a standard language what attributes and properties are to be inspected on IT systems. MACE developed SCAP content is frequently used to enable security operators to rapidly "spot check" an enterprise for the presence of malicious software. MACE has been used in the generation of SCAP content to address Threat Information Products and Threat Activity Reports from the Defense Industrial Base (DIB) Collaborative Information Sharing Environment (DCISE).

Ms. Ackerman is a Global Network Exploitation and Vulnerability Analyst in VAO. She has been supporting NSA, and the department's efforts, with SCAP production utilizing the MACE tool. Ms. Ackerman has a Bachelor of Science degree from Syracuse University, a National Defense Intelligence College, NDIC, Intelligence Diploma, and an Associate in Arts from San Diego Miramar College. Her career includes 22 years of military and civilian service.

Verification of SCAP Content – Harold Booth, NIST

In order to run properly in a broad range of SCAP-validated products, SCAP content needs to be built correctly and in accordance with the applicable specifications. The NIST SCAP Content Validation Tool is designed to validate the correctness of a SCAP data stream for a particular use case according to what is defined in NIST Special Publication 800-126. Harold will describe the use of the utility and will speak about challenges some organizations have experienced in creating / maintaining valid content.

Harold Booth is a Computer Scientist at the National Institute of Standards and Technology (NIST). Harold leads the development team for the National Vulnerability Database (NVD) and is also heavily involved in the development of the Security Automation Program specifications.

The MITRE Recommendation Tracker (RT) – Bryan Worrell, MITRE

This presentation will describe and demonstrate MITRE's Recommendation Tracker™ (RT) software, an open source program that facilitates development of automated security benchmarks. By automating the process of taking ordinary textual input, such as a typical system administrator might utilize, to create SCAP-compliant XCCDF output, RT makes the use of SCAP for inventory, compliance and vulnerability assessment tasks practical for a broad range of organizations.

Bryan Worrell is an InfoSec Scientist at MITRE and has worked in the Information Security field for the last three years. Bryan is currently leads the software development effort for both the Recommendation Tracker and XCCDF Interpreter. Bryan is also a member of the OVAL® Development team. Bryan attended Central Michigan University where he earned a Bachelor of Science degree in Computer Science.

SCAP Content Creation Solutions Using the eSCAPe Editor and Libraries – Peter Parker, G2

The Security Content Automation Protocol (SCAP) suite of specifications and protocols were developed to address a need by security professionals to exchange critical security information within the enterprise and the broader security community. SCAP compliant applications capable of leveraging SCAP to foster automated vulnerability management, policy compliance and malware detection have now been widely deployed. These tools rely on the availability of accurate and valid SCAP documents, often called SCAP content, to assess the security posture of managed systems. This content however can be difficult to generate and often represents the largest barrier to SCAP adoption. The Enhanced SCAP Editor (eSCAPe) provides a friendly interface for the creation of SCAP content that does not require extensive familiarity with SCAP. When content generated with eSCAPe is run on a NIST validated SCAP tool, what results is a transparent and scalable methodology for the detection of software vulnerabilities, configuration settings and malware infections.

Mr. Parker has extensive information assurance experience supporting both public and private sectors. Peter has performed system administration, systems hardening, software development and systems certification and accreditation of information systems and implemented data security measures. Peter is one of the leading engineers at G2 charged with developing specialized SCAP content, system assessment, group training and support for SCAP literacy, tool use and development.

Secure Configuration Management: DoD Use Cases for SCAP and Securing Configurations – Jim Shelton/Mike Kinney, NSA, Dave Hoon, DISA

The Secure Configuration Management (SCM) Program will provision the cyber warrior with pervasive enterprise abilities to collect, quantify, evaluate, understand, and act on information about the security configuration of every Department of Defense (DoD) cyber asset. Full deployment of the SCM system-of-systems will enable automated machine-to-machine reporting and command and control consistent with DoD requirements for centralized control, decentralized execution in support of both assured information

access to the warfighter and blue force readiness of the DoD cyber assets. The presentations will address how DoD is using SCAP and automation to Know what devices are on the networks, how they are configured, the risk level of those assets based on their configuration, remediation methods, and reporting and distribution of that information.

Jim Shelton is Portfolio/Program Manager, for Secure Configuration Management, in the Enterprise Security Management Special Projects Office (ESM SPO). Mr. Shelton serves as the DoD Lead for SCM under the Comprehensive National Cybersecurity Initiative (CNCI), working closely with the Defense Information Systems Agency (DISA), National Institute of Standards and Technology (NIST), CYBERCOM, and various DoD Components to enhance current Network and Agent Based DoD Security Systems to leverage SCAP standards and system interfaces that can automate the collection, assessment, and remediation.

Michael Kinney Is Lead Engineer, Network Assessments, Computer Network Defense Research & Technology Program Management Office (CND R&T PMO) Mr. Kinney has been Lead Engineer since November 2009, since arriving at NSA Mr. Kinney has served as an NSA contributor to the DoD Enterprise Information Assurance (IA)/CND Solutions Steering Group (ESSG) Technical Analysis Groups (TAG). Focus has been on Enterprise Risk Management, Enterprise Security Configuration Management, Secure Configuration Compliance, and Automated Enterprise Patch Management. Prior to his current assignment Mr. Kinney worked at Joint Systems Integration Center under US JFCOM as Principal IA Engineer under Contract with General Dynamics, (2007-2009), IA Assessments US Marine Corp NOC operations, IA Operations , Camp Lejeune, NC (2005-2007) Lead Radia Software Engineer Navy Marine Corp Intranet (NMCI) under contract with EDS, (2004-2005) with prior Software Distribution related positions at US Postal Service IT (1999-2004) Mr. Kinney has a Masters Degree in Information Technology with a specialization in Information Security from CAPELLA University of Minneapolis, Minnesota (2007) and holds Certified Information Systems Security Professional (CISSP) and Certified Ethical Hacker (CEH) certifications.

David Hoon is the lead of the Secure Configuration Management PMO at DISA PEO-MA. As the SCM PMO lead, he is responsible for the management and execution of the SCM and continuous monitoring program activities, which include the capabilities integration of HBSS Policy Auditor, HBSS Asset Publishing Service (APS), VMS, eMASS, ACAS, SCCVI, SCRI, ENMLDS, and IAVM Services. Prior to supporting PEO-MA, David Hoon worked as a contractor on the DISA STIG development team, as a STIG author and as the STIG Contract Project Lead.

Network Automation Track
Room 316/317

Network security continues to be mostly a manual process, worsened by the difficulties in the gathering information about users and activities on the network. Many enterprises have proprietary tools, ranging from DHCP servers to firewalls to authentication servers to malware scanners, which all have bits of information about users or endpoints. However, the ability to grasp the "big picture" has been absent. Network Automation track will address new and proven assessment capabilities, open standards initiatives aimed at automating integration of network security systems, and methods to detect attacks from inside and out.

Extending SCAP into the VMware virtual infrastructure – Robert Hollis, Threatguard, Chris Farrow, VMWare

As the adoption of virtualization continues to grow, the need to automate configuration management, assessment and remediation of VMware's infrastructure has become a mission critical requirement. Until now, organizations have had to leverage the DISA STIG for ESX Server with various manual process and COTS tools because an SCAP validation solution to address VMware did not exist. Between June and August, the work to extend the OVAL® schema to support VMware and submit for approval in SCAP v1.2 was accomplished. Join Rob Hollis from Threatguard and Chris Farrow from VMware to learn about the new SCAP v1.2 support for VMware including the translation of VMware's vSphere Hardening guide into SCAP, the plans for the first SCAP validated product for VMware and a demo of current prototypes

Mr. Hollis is the Director of Product Development for ThreatGuard, Inc. He started working with OVAL® in 2003 and has become the ThreatGuard technical lead for SCAP standards application and promotion. He has charted multiple advancements in SCAP, including reporting, deviation management, advanced reporting, and aggregation, and has recently applied this expertise to VMware cloud assessments.

Chris Farrow is currently the Director of VMware's Center for Policy & Compliance, an organization providing intelligence and expertise to unify internal, industry, and regulatory standards into a complete policy and controls framework. With nearly 20 years of experience in systems engineering and security, Chris' background crosses several industries including the US Marine Corps, healthcare, manufacturing, investment banking and software development. Most recently, Chris has held several positions at EMC including that of Senior Virtualization Strategist. Prior to VMware & EMC, Chris has held product management and engineering positions for several well known vendors including Configuresoft, NetIQ, Intrusion.com and BindView Corporation. Chris is an industry resource on the topics of security management, virtualization security and regulatory compliance, and has spoken at VMworld, RSA, SANS, Gartner, and Blackhat conferences. Chris is a SANS Community Instructor, SANS Local Mentor and courseware author. He holds the CISSP, GSEC and GCIH certifications.

Automated Network Security Assessments – Doug Dexter, Cisco

This presentation will describe how Cisco's Audit team automates security assessments for over 30,000 devices. The audit team has applied automation to scale up their capabilities, reduce manual labor spent on firewall and device configuration review, and dramatically increase speed and accuracy when reviewing one of the largest and most complex network environments in the world. The presentation shows that it is possible to visualize a complete global environment, understand relationships and dependencies, and uncover major problems and compliance issues before they are uncovered or exploited by others. Powerful results from new technology for identifying zones, breaking a global environment into manageable pieces, and for automated configuration analysis will be shown.

Doug Dexter has been with the Cisco Systems Corporate Information Security Department for ten years. During his tenure he has done everything from maintain the internal firewalls to lead architecture development for a variety of enterprise-wide solutions. As the Team Lead for Cisco's internal PKI deployment, he built a team of people and solutions to provide certificates and sign the production code for IP phones, call managers, and cable modems. For the past four years Doug has been Cisco's internal Audit Team Lead, responsible for a global team of auditors who handle Cisco's acquisitions, vulnerability assessments, and site assessments. Prior to working at Cisco, Doug was active duty in the US Army for 11 years and is currently a Major in an Army Reserve Information Assurance unit. He holds an MBA from the University of Texas at Austin with a concentration in Information Systems, Controls, and Assurance, and is a CISM, CISA, and CISSP-ISSMP.

TNC: Open Standards for Network Security Automation – Steve Hanna, Juniper Networks

In order to achieve widespread network security automation, we need open standards for integrating all manner of security systems. Fortunately, the Trusted Network Connect (TNC) standards are designed to solve just this problem. In fact, the TNC standards are the foundation for several of the other talks in this track. Come get an intro to the TNC standards and see them in action.

Steve Hanna is a Distinguished Engineer at Juniper Networks. As co-chair of the Trusted Network Connect Work Group in the TCG and the Network Endpoint Assessment Working Group in the IETF, Steve has a deep and broad understanding of network security. He is the author of many papers, an inventor or co-inventor on 34 issued U.S. patents, and a regular speaker at industry events.

Security Coordination with IF-MAP – Matt Webster, Lumeta

Network security management has traditionally been a largely manual process. This must change to deal with fast-paced attacks and keep costs in control. Automation is the only answer and the IF-MAP standard enables such automation. Come learn more about IF-MAP and see a demonstration as well.

Matt Webster has over 20 years experience in networking and network security. Since joining Lumeta in 2004, Webster has held a number of different roles; including Managing Consultant – International Markets, and Director of Sales Engineering. Currently, as the Director of Technology Alliances at Lumeta Corporation, Webster is focused on building strong technology partnerships that enable companies and government organizations to realize the benefits of product interoperability, as well as assisting in the development of go-to-market products with Lumeta's business partners. He is an active participant in the Trusted Computing Group. Prior to Lumeta, Webster acquired extensive experience in network operations, network design, security management and transformation/transition management. Webster was Global Network Operations Manager for AT&T supporting General Motors and Delphi Automotive. As well, Client Services Manager for BankOne (Chase).

Progress in Near-Real Time Attack Detection at the Platform Level – Dr. Bruce Gabrielson, Booz Allen Hamilton

Significant progress has been made during the past year to improve capabilities for detecting attacks, particularly insider threat attacks, using audit and audit like data. Where bandwidth, storage, and support for monitoring are limited, the detect first and then monitor approach represents a practical mitigation strategy. This presentation will address detection strengths, data normalization strategies, equipment and support needs, piloting activities, and the potential for future expansion using the techniques discussed.

Dr. Gabrielson is a security industry visionary who has both directed and performed research, problem solving and detailed technical analysis in the areas of weapons systems, secure communications systems, networked computer systems, sensitive databases and protected web sites. A hardware and software engineer with three patents in the telecommunications field and three technical books to his credit, Dr. Gabrielson has over 37 years experience in the information assurance and communications security field. He is currently the Lead Technical Advisor for the CND R&T PMO at NSA and is also the Technical Chair of DoD's Insider Threat Technology Advisory Group.

Innovative Uses of SCAP Track

Ballroom I

Vast majority of our cyber defenses are in effect pinned down by relatively mundane technical problems: missing patches; unenforced policies; poor configuration choices; and inconsistent security controls. Come and learn how SCAP is helping us get unpinned; reduce manual labor expenses while improving security posture; improve security behaviors through enabling continuous monitoring; automate scanning for policy compliance such as USGCB (U.S. Government Configuration Baseline – new name by OMB to replace FDCC starting with Windows 7, IE8 and later), FISMA (Federal Information Security Management Act), and others.

SCM 2007 Microsoft – Michael Tan, Microsoft

This session will introduce Microsoft Security Compliance Manager, a solution released 4/2010 and newly released security baselines and setting pack baselines that work with Microsoft Security Compliance Manager. The primary focus will be on advanced features in Microsoft Security Compliance Manager to demonstrate end to end user scenarios to use Microsoft security baselines to accelerate customers' ability to efficiently manage the security and compliance process for the most widely used Microsoft technologies. This session will also demonstrate how to use Microsoft Security Compliance Manager helping SCAP content authoring.

Michael Tan is a senior software design engineer at Microsoft and he is currently working on projects building a platform to help authoring and managing security compliance baselines for Microsoft products and extending the platform to enable customers to secure Microsoft products in their environment and make sure keeping in compliance. Michael has been working on many security products since he joined Microsoft 13 years ago. Michael started working in Security and Compliance team 4 years ago; has been focusing on security solutions for IT management; the part of the effort has been around supporting SCAP. Michael is on OVAL® board.

ISA VoIP Security Project – Tom Grill, VeriSign, Paul Sand, Salare Security

Automating security control evaluation will provide tremendous benefits to enterprises and public sector agencies by driving out large amounts of labor expense and reducing cyber risk through a persistent, increased cyber security posture. SCAP is a powerful solution that can do more than competing legacy methods such as scripting, telnet, SNMP, and element management systems in delivering an automated security control evaluation system. Results from the Internet Security Alliances Unified Communications Security Project's based on the application of SCAP to IP Phones and soft phone clients will be discussed in detail. Necessary evolution of SCAP to strengthen this approach will be presented.

Thomas Grill is an accomplished technology professional with over 18 years of experience leading data networking, telecom and security teams in fast paced, dynamic environments. As Technical Director at VeriSign, Thomas is recognized as its expert on the convergence of voice, video and data technologies for enterprises, Internet and telecommunications service infrastructures. In addition, Thomas is co-chair of the VoIP Security working group for Internet Security Alliance. Prior to joining VeriSign, Thomas was Director of Network Engineering at Pathnet Telecommunications and Manager of Internet Engineering at Sprint. Thomas also held a variety of engineering and development positions at 3Com and Raytheon.

Paul Sand is a recognized telecommunication and Information Technology security expert. He was a contributor to The Financial Management of Cyber Risk report published by ANSI's Homeland Security Standards Panel (HSSP). He served as the Working Group Chairman of the UC Security Project at the Internet Security Alliance (ISA) and was the editor of the ISA's Applicability of the Security Control Automation Protocol (SCAP) to Voice over Internet Protocol (VoIP). Paul has advised the National Security Agency (NSA) and Defense Information Services Agency (DISA) on IP Telephony (IPT) security for their respective published IPT security guidance. He is an officer of the Board of Directors of the FBI InfraGard Chicago Chapter; a member of the US Secret Service Electronic Crimes Task Force (ECTF), and a member of the VoIP Laboratory Advisory Board at the Illinois Institute of technology. Paul has led research for the US Army Research Office in the area of covert communication channel defense.

Threat Assessment and Continuous Risk Dashboard/Risk Scoring – Kim Watson, NSA, Dr. George Moore, Dept. of State

Department of State has implemented a Continuous Monitoring Risk Dashboard/Risk Scoring Program that has had the desired effect of incorporating security into day-to-day network management activities. They are currently demonstrating that if the Risk Dashboard contains the appropriate set of findings, includes threats associated with those findings, and can account for implementations of controls meant to address the threats and/or findings, then this same dashboard can feed a more timely and accurate Certification and Accreditation (C&A) process. SCAP standards, content, and capabilities are foundational to the success of this improved C&A process. In this talk, DoS will discuss the operational problem they are addressing and the resultant value to the organization. NSA will discuss the incorporation of SCAP into this capability, sharing practical concerns and experiences of using SCAP to support these types of risk decision processes.

Ms. Kim Watson is the Technical Director for Information Analysis Transformation in VAO. She has been at NSA for over 20 years, most of which has been spent in VAO or one of its predecessor organizations. For the last 6 years Ms. Watson has been performing

analysis of network data, with a focus on how to represent and relate different aspects of the network security environment (e.g., vulnerability, threat, impact). Her goal is to help define the standards, models, and frameworks required to support and enable more accurate and actionable risk decisions.

Dr. George C. Moore has worked for several Federal agencies in the area of foreign affairs since 1973 including the US Peace Corps (2 years), USAID (22 years, four of them as a Research Associate from Johns Hopkins University), and the Department of State (3 years). He has also worked as an independent consultant (2 years), lead the formation of information system management program for both graduate and undergraduate students (5 years) in the early 1980s. Dr. Moore joined the Department of State team in November 2006 as the Chief Computer Scientist working directly for the Chief Information Security Officer. He was a key member of the team at State that raised the Department's IT Security grade from an F to a B (and USAID from F to A+) as assessed by OMB and Congress, while cutting costs (by 62% at State). His focus was on being an agent of change and finding simple, smart and direct ways to both comply with FISMA and OMB requirements and improve security

Automated Creation of SCAP Content –Peter Guerra and Shane Shaffer, G2

We have developed infrastructure for the automated acquisition and analysis of malware. A major component of this analysis is the automated production of SCAP content that specifies registry and file system modifications that are made by malware to the underlying operating system post-infection. Using the results of this analysis, it is possible to ask highly targeted questions over a population of end point systems in order to accurately determine whether they are infected with particular malware instances. For example, the Zeus v2 trojan creates the file "%system%\lowsec\user.dl.lll", and hence an SCAP-enabled scanner such as ovald can detect whether a system is participating in a Zeus v2 botnet by looking for this file. The ability to go from malware acquisition through the production of SCAP content in a automated fashion is a key enabler for the cyber analytic defense mission.

Peter Guerra is currently working as a security consultant to government organizations as a director at G2, Inc. His diverse IT career has focused on cyber crime, malicious code analysis, incident response, web application hacking, and security operations. He is currently getting his MBA and studying the relationship between economics and information security as related to cyber crime.

Shane Shaffer is the Technical Director of Security Automation at G2, Inc., a Columbia, Maryland-based firm committed to protecting our Nation's interests in Cyberspace. Splitting his time between the Massachusetts Institute of Technology and the University of Maryland College Park, Mr. Shaffer holds a BS in Computer Science. Mr. Shaffer has focused his career on the field of enterprise security management, serving as the former lead architect of the Department of Defense Vulnerability Management System. A staunch advocate of security automation, Mr. Shaffer has been a key contributor to the development of SCAP from the inception of its individual component standards. Mr. Shaffer remains active in specification development and implementation of security automation systems through his work for national security clients.

SCAP Compliance Checker: Developing a Government-Funded SCAP Validated Application – Jack Vander Pol, SPAWAR

The SCAP Compliance Checker (SCC) is the only federally funded, SCAP Validated, FDCC scanner. Since its original release, developed for the Internal Revenue Service, it has been adopted by numerous federal agencies and contractors. Following a recent joint collaboration with the National Security Agency, an updated version of SCC will soon be released. This presentation will include a brief history of our application, who can use it, and a software developer's perspective on the benefits and challenges of following the SCAP framework. A demonstration of the latest version of the SCC, highlighting the implementations of OVAL® 5.7 and Cyberscope, will be included.

Mr. Jack Vander Pol is a Computer Scientist at the Space and Naval Warfare (SPAWAR) Systems Center Atlantic in Charleston, SC, where he is responsible for the project management of the SCAP Compliance Checker, as well as other scanners for Unix, Windows, mainframes, and Cisco routers. Prior to project management and software development, Mr. Vander Pol performed five years of Security Tests and Evaluations for federal agencies. Mr. Vander Pol holds a B.A in Mathematics from the Southwest Minnesota State University.

Leveraging SCAP for TNC, Endpoint Sensor Grid and Automated Remediation – Jim Ivers, Triumfant

Triumfant was an early adopter of SCAP and has leveraged the standards throughout the Triumfant solution. This presentation will provide practical examples of innovative uses of SCAP by using specific use cases:

- Implementing an endpoint sensor grid and using the detailed data from the grid for advanced vulnerability reporting.
- Implementing a working model of the "comply to connect" concept using the Trusted Network Connection (TNC) architecture that is part of the larger Trusted Computing Group (TCG) architecture.
- Implementing automated remediation for continuously enforcing security configurations.

The presentation will address the practical benefits of each one of these use cases, explore the actual implementation, and define how SCAP is leveraged in each use case to facilitate the sharing of information.

Mr. Jim Ivers is the Chief Security Strategist for Triumfant where he is responsible for product management of the Triumfant

solution. Mr. Ivers was previously on the executive team of Cybertrust, a worldwide security services company sold to Verizon Business. Prior to Cybertrust, Mr. Ivers played a key role in transforming webMethods from a proprietary integration company to a standards-based service oriented architecture company (SOA). He also has a background in business intelligence and data warehousing. Mr. Ivers holds a B.S. in Computer Science from the University of Central Florida.

Security Management and Compliance Automation Track
Room 318/319

Through use cases, and management and technical discussions, the Security Management and Compliance Automation track will explore how security automation tools, technologies, and specifications support critical security capabilities, such as Continuous Monitoring and Configuration Management; facilitate compliance and reporting with important security and privacy laws and regulations, such as FISMA, HIPAA, and the HITECH Act; and enable the sound security management practices necessary to secure the mission in today's volatile threat environment.

IT Security: Tying the Pieces Together – Mischel Kwon, RSA

IT Security – Compliance? Security Operations? Configuration Management? Vulnerability Management? Threat Management? Data Management? Identity Management? We understand the need for all these function to achieve IT Security, but do we understand how these function work together? What metrics and reporting are needed throughout the organization to make these efforts meaningful? Can we track the workflow needed to fix vulnerabilities? Can we make compliance reflective of today's attacks? Learn how IT Security is really Security Management: managing the metrics, data and tasks needed to keep ahead of the threats and attacks while ensuring all levels of management that the work is being done to keep the mission secure.

Mischel Kwon is Vice President and CTO of Public Sector Security Solutions for RSA, The Security Division of EMC. In this role, Ms. Kwon is responsible for leading RSA in assisting the public sector security solutions, strategies, technologies and policy. Ms. Kwon has more than 27 years of experience, with expertise and leadership in the design, implementation and management of critical IT infrastructure and security operations programs. Prior to joining RSA, Ms. Kwon was the Director for the United States Computer Emergency Readiness Team (US-CERT), where she spearheaded the organization responsible for analyzing and reducing cyber threats and vulnerabilities in federal networks, disseminating cyber threat warning information and coordinating national incident response activities. In addition, she previously served as the Deputy Director for IT Security Staff at the United States Department of Justice (DOJ), where she built and deployed the Justice Security Operations Center (JSOC) to monitor and defend the DOJ network against cyber threats. Since 2006, Ms. Kwon has served as Adjunct Professor of Cyber Defense and leads the Cyber Defense Lab at George Washington University. She holds a Master of Science in Computer Science and a graduate certificate in Computer Security and Information Assurance.

Introduction to CyberScope – Alfredo Rohweder

This session will provide an overview of Cyberscope, its role in facilitating the manual and automated reporting of agency data for FISMA and information security.

Alfredo Rohweder is the lead developer for DHS's CyberScope application that is transforming information security reporting from a compliance paper-based model to a data-centric, performance-based focus and continuous monitoring. Mr. Rohweder is a graduate of James Madison University, and has over 25 years experience designing and implementing innovative automated solutions for a wide range of clients from industry, DoD and Civil agencies.

Client Technologies that Help Assist with Security and Privacy Regulation Compliance – David Houlding, Intel Heath

The digitization of the US healthcare system is a critical part of lowering healthcare costs, improving patient outcomes, and increasing access to services. While some organizations are far along in their journey towards fully digitized and integrated workflows, others are just taking their first steps towards digitization. No matter where your organization is at on the continuum of digitization, compliance with federal security and privacy regulations in the form of HIPAA and HITECH is a significant concern. This session will provide a brief overview of these two regulations and discuss technology solutions that can help ease the path to compliance as well as provide a better end-user experience. Specifically, Intel vPro Technology, Intel Antitheft Technology, hardware-based acceleration of data encryption, and client strategies which utilize virtualization will be reviewed.

David Houlding is a Healthcare Enterprise Architect at Intel Health with over 18 years of experience in enterprise architecture and security. As the lead security architect for the Intel Health Guide System, David has extensive experience in healthcare information systems security. He also has experience across a variety of other business domains including financial services, manufacturing, telecommunications, insurance, satellite imaging, and research and development. With several patents granted by the USPTO, David has a proven track record for innovation. He has a Master of Applied Science in Data Compression and Digital Signal Processing from Simon Fraser University, British Columbia, Canada. David has presented and participated in panel discussions at numerous major industry conferences including Enterprise Architecture Practitioners Conferences, Innovation Insights, ECommerce World, Wireless One and Java Development conferences. He has also published numerous articles in major trade journals including

"Dr. Dobb's Journal," has made contributions to book publications including "XML Unleashed," and has been interviewed for newspaper and other articles.

Continuous Monitoring Panel – Peter Mell (moderator), COL Michael Jones, HQDA, John Streufert, DOS, Tim McBride, DHS

The overarching objective of a continuous monitoring program is to determine if the complete set of security controls within an information system or inherited by the system continue to be effective over time in light of the inevitable changes that occur. This technology-focused panel session will discuss the role of automation in continuous monitoring solutions, as well as the outputs of the ISIMC Continuous Monitoring Working Group.

This session will take a deep dive into foundational elements to enable technical continuous security monitoring. It will start from a definition and then derive essential characteristics. It will then take an enterprise architecture view and drive down through technical architectures to necessary components, interfaces, and communication models. The session will end discussing needed requirements and validation programs to enable continuous monitoring implementations within government.

Peter Mell is a senior computer scientist in the Computer Security Division at the National Institute of Standards and Technology (NIST). He is currently researching continuous security monitoring and related security automation capabilities. His past work includes creating the U.S. National Vulnerability Database, co-founding the NIST Security Content Automation Protocol (SCAP), and creating the SCAP product validation program. He was also the lead author of the Common Vulnerability Scoring System (CVSS) vulnerability metric used to secure credit card systems worldwide and he initiated the Federal Risk and Authorization Management Program (FedRAMP) for enabling government-wide risk management of large outsourced and multi-agency systems. His research experience includes the areas of cloud computing, security metrics, security automation, vulnerability databases, and intrusion detection systems.

COL Michael Jones has over 26 years of military service. Since 1995 all his military assignments were related to information technology. From 2000 - 2004 he operated the Army National Guard's worldwide network known as GuardNet. He has served in many senior IT management positions to include: Chief, IT Plans and Policy; Deputy Director of the Enterprise Technology Service Activity and as the Deputy Director Cyber - Emerging Technologies. He holds the Information Technology Infrastructure Library (ITIL) foundation certification, is a Lean Six Sigma green belt and has completed the Chief Information Officer (CIO) course with Information Assurance (IA) emphasis from the National Defense University. He has a Bachelor of Arts Degree in Math education from the University of Central Florida and a Master of Science degree in Information Resource Management from Central Michigan University.

John Streufert joined the Department of State in July 2006 as the Chief Information Security Officer. Closing a material weakness and raising measures of IT security performance mark his tenure. Since arriving at State he lowered a material weakness on IT Security to a deficiency and raised the IT Security grade from an F to a B as assessed by OMB and Congress. In July 2008 at Mr. Streufert's request, the Department began providing letter grades monthly to executives and technical managers on progress in lowering IT security risk based on correcting scanned vulnerabilities and configuration weaknesses. In 2010 Mr. Streufert was named Chief Information Security Officer of the Year by Government Executive magazine. Mr. Streufert has also served as the Acting CIO for the Agency for International Development from 2003-2006, and as the Director of Information Resources Management for the Federal Crop Insurance Corporation, the Naval Shipyards and the Naval Sea Systems Command. Mr. Streufert was a graduate of the Maxwell School of Public Affairs, Syracuse University (MPA) in 1985 and St. Olaf College (B.A.) in 1979.

Mr. McBride has 15 years of experience managing, developing, and deploying information technology and security solutions in the Federal and Commercial environments. Currently Mr. McBride enhances the financial and security posture of the Federal IT landscape through consolidating essential services in the Department of Homeland Security's, Requirements and Acquisition Services Program supporting the National Cyber Security Division's Federal Network Security Branch. Mr. McBride holds a BA from the University of Hawaii, an MS from The George Washington University and is a Certified Project Management Professional (PMP).

Configuration Management – Kelley Dempsey, NIST

NIST recently released the first public draft of Special Publication (SP) 800-128, *Guide for Security Configuration Management of Information Systems*, which provides foundational guidance on integrating security configuration management into an organization's overall information system security program. More specifically, the publication elaborates on the application of the Configuration Management family of security controls from SP 800-53 and provides guidelines for managing the configuration of system and enterprise architecture and associated components for secure processing, storing, and transmitting of information. SCM supports integration of SCAP-enabled automated tools into an enterprise and plays a crucial role within the NIST Risk Management Framework (RMF). This session provides an overview of SP 800-128 and the RMF and details how implementation of SCM supports the RMF and information system security in general.

Kelley Dempsey began her career in information technology in 1986 as an electronics technician repairing PCs and printers before moving on to system administration and network management throughout the 1990s. While employed by the Department of the Navy in 1999, she began focusing on information system security by training for and conducting large scale DITSCAP system accreditations from start to finish. Kelley and her husband moved to the DC area from California in the spring of 2001 and Kelley joined the NIST operational Information Security team, managing the NIST information system C&A program through September

2008. Kelley joined the NIST Computer Security Division FISMA team in October 2008, co-authored NIST SP 800-128 Security Configuration Management (draft) and is a co-author on the upcoming NIST SP 800-137 Continuous Monitoring Guidance (working title only). Kelley has also been a major contributor to NIST SPs 800-53 Rev 3, 800-37 Rev 1, and 800-53A Rev 1. Kelley completed a B.S. degree in Management of Technical Operations from Embry-Riddle Aeronautical University, graduating cum laude in December 2003 and maintains a CISSP certification earned in June 2004.

FISMA Automation in a Global Enterprise – Earnest Neal, Atlantic Systems Group, Inc., Dirk Barrineau, VA

This session will cover all six steps of the Risk Management Framework (RMF) and how to efficiently and effectively implement the RMF for any size organization. A centralized process will be demonstrated that walks an organization through the RMF and will hit on real world topics such as penetration testing, application scanning, vulnerability scanning, 1/3rd control selection and system configuration scanning (SCAP/FDCC).

Mr. Neal has 14 years of experience in the Information Security industry. He is an experienced consultant with proven capabilities and strong information security and system solutions background. Before joining ASG, Mr. Neal was a member of e-Security and ISS X-Force Professional Security Services team. While at ISS Mr. Neal planned and managed many network designs efforts across the federal government. Over the past 5years Mr. Neal has been focused on the Certification and Accreditation arena across DOD and the Federal Civilian sectors. Mr. Neal has managed over a 1000 Certification and Accreditation efforts following NIST's Risk Management Framework for the FISMA process.

Mr. Barrineau was named the Deputy Director for Operations, Certification Program Service in January 2008. He is responsible for the communication, coordination and onsite security control assessments for Veterans Affairs certification and accreditation (C&A) effort. Mr. Barrineau has also developed customer service models used in other projects in VA and has received numerous awards for his efforts in service to clients and stakeholders across VA. Prior to joining VA (07/2004), Mr. Barrineau worked various information projects as a member of the National Association of Securities Dealers Automated Quotations (NASDAQ) and in the bio-technology company QIAGEN. Mr. Barrineau also served in the US Air Force and currently resides in Martinsburg, West Virginia.

Security Automation For Cloud Computing Track

Room 321-323

This track will focus on how to apply the area of security automation to cloud computing. It begins with an in-depth cloud security keynote followed by a focus on security for private clouds, continuous monitoring for clouds, and creation trustworthy cloud systems.

Cloud Security Opening Address – Peter Mell, NIST, Dennis Moreau, RSA

This session will take a deep dive into foundational elements to enable technical continuous security monitoring. It will start from a definition and then derive essential characteristics. It will then take an enterprise architecture view and drive down through technical architectures to necessary components, interfaces, and communication models. The session will end discussing needed requirements and validation programs to enable continuous monitoring implementations within government.

Peter Mell is a senior computer scientist in the Computer Security Division at the National Institute of Standards and Technology (NIST). He is currently researching continuous security monitoring and related security automation capabilities. His past work includes creating the U.S. National Vulnerability Database, co-founding the NIST Security Content Automation Protocol (SCAP), and creating the SCAP product validation program. He was also the lead author of the Common Vulnerability Scoring System (CVSS) vulnerability metric used to secure credit card systems worldwide and he initiated the Federal Risk and Authorization Management Program (FedRAMP) for enabling government-wide risk management of large outsourced and multi-agency systems. His research experience includes the areas of cloud computing, security metrics, security automation, vulnerability databases, and intrusion detection systems.

Dennis Moreau is specialist in the application of leading edge technologies to the solution of complex problems in the Information Systems and Utility Computing management domains. His primary focus is in developing enterprise scale solutions to improve efficiency and effectiveness for security, compliance and configuration management. He works actively with NIST, the DoD and the Mitre Corporation on the development of security configuration policy compliance standards. He has over than 35 years of experience design, evaluation and management of operations and security infrastructures. Prior to joining RSA's CTO Office, he was a founder and the Chief Technology Officer for Configuresoft. He has also been the Associate Vice President for IT and Chief Technology Officer for Baylor College of Medicine (BCM). He holds a doctorate in Computer Science and has held faculty positions in Computational Medicine and Computer Science. Dr. Moreau speaks regularly at IT management and security conferences worldwide.

Security Automation in Private Clouds Panel – Neil Ziring, NSA (moderator), Mischel Kwon, RSA, Steve Orrin, Intel, Jen Nowell, Symantec, Gregg Brown, Microsoft

This panel will discuss the specific security automation needs of private cloud computing. The goal is to assist agencies in understanding how to build private clouds in a secure way that will enable use of cloud computing for higher sensitivity data.

Mischel Kwon is Vice President and CTO of Public Sector Security Solutions for RSA, The Security Division of EMC. In this role, Ms. Kwon is responsible for leading RSA in assisting the public sector security solutions, strategies, technologies and policy. Ms. Kwon has more than 27 years of experience, with expertise and leadership in the design, implementation and management of critical IT infrastructure and security operations programs. Prior to joining RSA, Ms. Kwon was the Director for the United States Computer Emergency Readiness Team (US-CERT), where she spearheaded the organization responsible for analyzing and reducing cyber threats and vulnerabilities in federal networks, disseminating cyber threat warning information and coordinating national incident response activities. In addition, she previously served as the Deputy Director for IT Security Staff at the United States Department of Justice (DOJ), where she built and deployed the Justice Security Operations Center (JSOC) to monitor and defend the DOJ network against cyber threats. Since 2006, Ms. Kwon has served as Adjunct Professor of Cyber Defense and leads the Cyber Defense Lab at George Washington University. She holds a Master of Science in Computer Science and a graduate certificate in Computer Security and Information Assurance.

Steve Orrin is Director of Security Solutions, for SSG's SPI group at Intel, Corp. and is responsible for Security Strategy and Pathfinding. Steve joined Intel as part of the acquisition of Sarvega, Inc. where he was their CSO. Steve was previously CTO of Sanctum, a pioneer in Web application security testing and firewall software. Prior to joining Sanctum, Steve was CTO and co-founder of LockStar, Inc. LockStar provided enterprises with the means to secure and XML/WebService enable legacy mainframe and enterprise applications for e-business. Steve joined LockStar from SynData Technologies, Inc. where he was CTO and chief architect of their desktop e-mail and file security product. Steve was named one of InfoWorld's Top 25 CTO's of 2004 and is a recognized expert and frequent lecturer on enterprise security. Steve is a member of the Information Systems Audit and Control Association (ISACA), the Computer Security Institute (CSI), International Association for Cryptographic Research (IACR) and is a co-Founder of WASC (Web Application Security Consortium) and a Co-Founder of the SafeSOA Taskforce. Steve was named a fellow at the Center for Advanced Defense Studies.

Jennifer Nowell manages the Government Solutions Group for Symantec Public Sector. In this role, Ms. Nowell leads strategic functions associated with Symantec's Public Sector business – working with US Federal, State, and Local governments as well as education institutions to improve their ability to protect and manage critical information. She brings comprehensive and long-term security solutions to the US Public Sector in cooperation with government organizations, integrators, and other leading security vendors.

Continuous Monitoring for Cloud Panel – Peter Mell, NIST, Christopher Hoff, Cisco, Kent Landfield, McAfee

Technical continuous security monitoring is a current focus area in the security community as is cloud computing. This panel will combining these subjects and discuss how one can automate the security management of cloud implementations.

This session will take a deep dive into foundational elements to enable technical continuous security monitoring. It will start from a definition and then derive essential characteristics. It will then take an enterprise architecture view and drive down through technical architectures to necessary components, interfaces, and communication models. The session will end discussing needed requirements and validation programs to enable continuous monitoring implementations within government.
Peter Mell is a senior computer scientist in the Computer Security Division at the National Institute of Standards and Technology (NIST). He is currently researching continuous security monitoring and related security automation capabilities. His past work includes creating the U.S. National Vulnerability Database, co-founding the NIST Security Content Automation Protocol (SCAP), and creating the SCAP product validation program. He was also the lead author of the Common Vulnerability Scoring System (CVSS) vulnerability metric used to secure credit card systems worldwide and he initiated the Federal Risk and Authorization Management Program (FedRAMP) for enabling government-wide risk management of large outsourced and multi-agency systems. His research experience includes the areas of cloud computing, security metrics, security automation, vulnerability databases, and intrusion detection systems.

Christopher Hoff is Director of Cloud & Virtualization Solutions at Cisco Systems where he focuses on virtualization and cloud computing security, spending most of his time interacting with global enterprises and service providers, governments, and the defense and intelligence communities. Previously, he was Unisys Corporation's Chief Security Architect, served as Crossbeam Systems' chief security strategist, was the CISO and director of enterprise security at a $25 billion financial services company and was founder/CTO of a national security consultancy amongst other startup endeavors. Hoff is interviewed regularly by the media and press, is a featured guest on numerous podcasts and has keynoted and presented at numerous high-profile security conferences including Black Hat, DefCon, Microsoft's Bluehat, Source, SecTor, FIRST, SANS and Troopers. Hoff is a founding member and technical advisor to the Cloud Security Alliance, founder of the CloudAudit project and the HacKid conference and blogs at http://www.rationalsurvivability.com/blog. Hoff is a CISSP, CISA, CISM and NSA IAM. He was twice nominated as the Information Security Executive of the Year and won the Security 7 award in Financial Services in 2005. Hoff is a 2010 Microsoft MVP (Security) and a 2010 VMware vExpert.

Kent Landfield has spent over 25 years in software development, global network operations and network security arenas. He has recently taken on the responsibility of Director of Content Strategy, Architecture and Standards in McAfee® Labs. Before this, Kent managed the global Risk and Compliance Security Research teams at McAfee. His responsibility included producing the content supplied with McAfee's remediation, policy auditing, vulnerability management and NAC products. Kent was a catalyst in getting SCAP component standards adopted as the basis for product and content integration across three different technologies within McAfee. He initiated the first large scale commercial SCAP Content development team and content production architecture in the world. His team achieved the first localization of SCAP content, delivering completely localized content in eleven languages enabling SCAP products to be sold into a true global market. Kent has been involved with the development of security standards since the POSIX working groups in the late 1980s. He has also been involved with standards development in the Internet Engineering Task Force and Trusted System Interoperability Groups. He was one of the initial CVE® Editorial Board Members and is also an OVAL® Board member, a CPE™ Core Team member and is active in the emerging standards working groups.

Creating Trustworthy Cloud Systems – Ron Knode, CSC and Steve Orrin, Intel

This session will discuss emerging technologies that will enhance cloud security capabilities through security automation methodologies. A specific focus will be on technologies that enhance the underlying trustworthiness of cloud components.

Ron Knode is a Director in the Global Security Solutions (GSS) business unit of CSC. In 2006 Ron was also named a Research Associate in CSC's internal "innovation think tank", known as the Leading Edge Forum (LEF). Today, he serves in both roles for CSC, bringing the innovation ideas and approaches uncovered in research to practical application in security services and technologies.

Steve Orrin is Director of Security Solutions, for SSG's SPI group at Intel, Corp. and is responsible for Security Strategy and Pathfinding. Steve joined Intel as part of the acquisition of Sarvega, Inc. where he was their CSO. Steve was previously CTO of Sanctum, a pioneer in Web application security testing and firewall software. Prior to joining Sanctum, Steve was CTO and co-founder of LockStar, Inc. LockStar provided enterprises with the means to secure and XML/WebService enable legacy mainframe and enterprise applications for e-business. Steve joined LockStar from SynData Technologies, Inc. where he was CTO and chief architect of their desktop e-mail and file security product. Steve was named one of InfoWorld's Top 25 CTO's of 2004 and is a recognized expert and frequent lecturer on enterprise security. Steve is a member of the Information Systems Audit and Control Association (ISACA), the Computer Security Institute (CSI), International Association for Cryptographic Research (IACR) and is a co-Founder of WASC (Web Application Security Consortium) and a Co-Founder of the SafeSOA Taskforce. Steve was named a fellow at the Center for Advanced Defense Studies.

The Need for Software Security Assurance to Secure Mission Critical Applications in the Federal Cloud – Rob Roy, Fortify

Hackers are targeting applications as their new way "in"; and, as a result, businesses and the cloud infrastructure providers that support them must proactively identify and resolve security vulnerabilities that reside in applications. Government agencies can only be assured that their mission critical applications are secure in the cloud if their service provider makes it a priority to apply application security best practices, including ongoing vulnerability testing and remediation and management.

Rob is currently the Federal Chief Technology Officer at Fortify Software. In this capacity, he represents Fortify's technology leadership to Government, Systems Integrator and Critical Infrastructure organizations seeking to address their Software Security Assurance challenges. Rob brings a unique perspective to his role at Fortify. After 10 years in the US Navy managing computing infrastructures, communications and cryptography, he adopted a core belief in using technology to improve human challenges. He experienced that it could be applied to a strong defense, as well as to opening lines of communication during crisis situations. His transition to the private sector focused on both early stage startups as well as large established vendors including IBM, Microsoft and Oracle; companies that offered solutions in the fields of security, communications, visualization and situational awareness to organizations with complex missions, challenging physical environments, and a critical need to improve their operational stance. Rob caught the humanitarian bug during the national and international disasters of 2004 and 2005, when he coordinated Microsoft efforts to use technology after hurricane Katrina, the Asian Tsunami, and Pakistan earthquake to help Defense and NGO organizations manage displaced populations, triage health requirements, direct needed supplies, and restore general communications to the affected regions. He believes that protecting information at the application level is the last line of defense in a never-ending cyber threat that is increasing in both sophistication and harm to the international community. Rob studied mathematics and computer science at the US Naval Academy.

Standards to Acceleration to Jumpstart Adoption of Cloud Computing – Lee Badger and Chris Johnson, NIST

The basic concepts of cloud computing date from the 1960s and utility computing, but those ideas have new relevance today with the increasingly effective use of fast networks and efficient virtualization techniques to enable practical rentals of computing resources accessed over network connections. Computing rentals are extremely convenient for many uses but raise significant computer security issues: how can cloud computing customers be confident that their workloads are securely hosted? This presentation will briefly review the essentials of cloud computing, focusing on the NIST definition of cloud computing. It

will then consider security in the cloud, from the viewpoint of key management (briefly) and from the viewpoint of virtualization. The presentation will illustrate the connections between cloud computing and the need for automated security monitoring via frameworks such as SCAP. The presentation will then introduce a new NIST project in cloud computing: Standards Acceleration to Jumpstart Adoption of Cloud Computing (SAJACC) and discuss the ambitions of the SAJACC project to foster cloud computing standards that provide portability of user workloads, interoperability among cloud providers, and support for security.

Lee Badger is a computer scientist at the National Institute of Standards and Technology (NIST). Mr. Badger has over 20 years of experience with computer security research, with a focus on operating system access control. Prior to joining NIST in 2008, Mr. Badger served as a Defense Advanced Research Projects Agency (DARPA) program manager for 6 years where he funded and managed a variety of programs focusing on self-regenerating systems, intrusion tolerance, self-defending applications, software security analysis, and software producibility. Prior to joining DARPA, Mr. Badger led development efforts culminating in implementations of Domain and Type Enforcement (DTE) for UNIX, a DTE-enforcing firewall, a Generic Software Wrappers system for UNIX, and application of software wrappers for intrusion detection. Mr. Badger holds an M.S. in Computer Science from the University of Maryland, College Park, awarded in 1987.

Christopher Johnson is a Computer Scientist at the National Institute of Standards and Technology (NIST) where he manages the National Vulnerability Database software flaw analysis activities, submissions to the National Checklist Program and hosting of Security Content Automation Protocol data sources. Prior to joining NIST, Mr. Johnson worked as consultant to Federal and State government agencies and the investment banking, securities and insurance industries. Mr. Johnson was a founder and principal of an information assurance practice that provided vulnerability assessment, security architecture design, code development, certification and accreditation, and security testing and evaluation services. His research interests include security automation, software flaw analysis, and security metrics.

SCAP Workshop
Ballroom I

The SCAP Workshop Track will consist of a series of workshops focused on evolving the specifications within the Security Content Automation Protocol (SCAP). These workshops will be similar to the workshops held during SCAP Developer Day events. The purpose of these workshops is for the community to discuss SCAP in technical detail and to derive solutions to current problems that benefit all concerned parties. These workshops will address both current and emerging SCAP specifications.

XCCDF – Charles Schmidt, MITRE

This workshop will cover some of the open issues that have been raised by the XCCDF community. There will also be an initial discussion of the nature of XCCDF 2.0 that will inform the planning of the next major release of the standard. This is intended to be an open discussion and an opportunity for members of the XCCDF community to provide feedback to the XCCDF development team. This workshop is for experienced XCCDF and/or SCAP users and developers in order to provide a forum for them to share their experiences and insights into the design of XCCDF.

Charles Schmidt is a Lead Information Security Engineer at the MITRE Corporation. He has supported security guidance development efforts for more than 10 years covering a wide range of technologies. He has directly supported the CVE®, CCE™, OVAL®, and OCIL security automation standards and is currently the moderator of the XCCDF benchmark standard. He also led the development teams for a number of supporting applications including the Windows Investigator Tool and the Benchmark Editor. Charles holds a Bachelors degree in both Mathematics and Computer Science from Carleton College and a Masters degree in Computer Science from the University of Utah.

Vulnerability Data Model – Harold Booth, NIST

The National Vulnerability Database (NVD) provides publically accessible, XML-based vulnerability data feeds. These feeds are currently based on an XML Schema developed within the NVD to provide a machine-readable format of the NVD CVE® data. In an effort to improve security automation NIST is undergoing an effort to standardize the Vulnerability Data Model behind these feeds to allow tools and organizations to disseminate vulnerability data in a standardized way. Standardization in the exchange of vulnerability data will enable a wide variety tools and organizations to share and process vulnerability data. This workshop will begin with an overview of the draft Vulnerability Data Model. The remaining workshop is designed to solicit feedback from community members interested in helping to form and improve the vulnerability model.

Harold Booth is a Computer Scientist at the National Institute of Standards and Technology (NIST). Harold leads the development team for the National Vulnerability Database (NVD) and is also heavily involved in the development of the Security Automation Program specifications.

OVAL® Future Considerations – Jon Baker, MITRE

This workshop will explore the need for a major revision to the OVAL® Language. A number of possible capabilities will be discussed with the goal of gathering community feedback and understanding both the need for any changes and their impact.

Jon Baker is a Lead Information Security Engineer at the MITRE Corporation. He currently leads the OVAL® team at MITRE and has spent the past seven years working with colleagues, industry, and government participants to develop open community standards for security automation. During this time Jon's various roles included leading the development of the OVAL® Interpreter and the OVAL® Repository infrastructure, collaborating with the standards community to evolve the OVAL® Language, and contributing to the CPE™, OCIL, XCCDF, and SCAP efforts. Jon holds a Bachelors degree in Psychology from Tufts University and a Masters degree in Computer Science from Boston University.

ARF – John Wunder, MITRE, Adam Halbardier, BAH

ARF (Asset Reporting Format) is an emerging security automation standard that will support reporting on the results of asset assessments. In combination with an asset identification specification, ARF is being proposed for inclusion in SCAP 1.2 to support reporting on the results of SCAP assessments. The intent of this workshop is to get feedback from the community, in particular vendors and end users of security assessment products, to ensure that ARF and the asset identification specifications best meet the community's needs.

John Wunder is a senior software systems engineer at The MITRE Corporation who has been active in the security automation community for several years, supporting SCAP content development, security interface specifications, remediation standards, and asset management. His other work at MITRE includes support to government customers performing cyber command and control and mission assurance. He received his Bachelors in Computer Science at St. John's University and his Masters in Information Assurance at Northeastern University.

Adam Halbardier is a security professional and software engineer working for Booz Allen Hamilton. He supports the National Institute of Standards and Technology (NIST) Security Automation Program. Specifically, Mr. Halbardier developed the Security Content Automation Protocol (SCAP) Schematron rules for the SCAP Content Validation Tool, and he now maintains that tool. He is also coauthor of NIST Interagency Report (IR) 7693 – Asset Identification and NIST IR 7694 – Asset Reporting Format. Mr. Halbardier has a Bachelor's Degree in Computer and Electrical Engineering from the University of California, Irvine.

EMAP Workshop
Room 316/317

The EMAP Engineering Workshop is open session where information about the EMAP effort will be exchanged. Community feedback and input is sought to drive requirements and other considerations.

Event Management Automation Protocol (EMAP) Status Update

The EMAP session will describe the progress and goals of the EMAP specification to date and highlight activity and plans for the future. This an open discussion to solicit feedback and community guidance for the specification overall.

Open Event Expression Language (OEEL) Engineering Session

OEEL is intended to reduce the complexity of acquiring log sources and to standardize and externalize the expression of log parsing logic for data exchange and reusability purposes. The OEEL session will describe the concepts and notional design elements in the proposal for the OEEL specification. The focus will then shift to use cases, and applicable scenarios for the use of the language. This an open discussion to solicit feedback and community guidance for the specification

Common Event Rule Expression Engineering Session

CERE is intended to standardize the way in which rules for log correlation, pattern analysis, and filtering are expressed as a exchange format. Research into the use of the Rules Interchange Format (RIF) from W3C and other existing specifications as a vehicle for rule expression will be highlighted. The CERE session will then focus on describing the concepts and notional design elements in the proposal for the CERE specification. The focus will then shift to use cases, and applicable scenarios for the use of the language. This an open discussion to solicit feedback and community guidance for the specification.

Emerging Topics

This session will allow for discussion of topics that are related to EMAP and may be candidate components, as well as to identify gaps or new developments that may be relevant to the effort. Topics such as the Comment Event Expression (CEE), Common Attack Pattern Enumeration and Classification (CAPEC™), and Malware Attribute Enumeration and Characterization (MAEC™) will be discussed and additional suggestions or feedback solicited from the audience.

Remediation Workshop
Room 321-323

The Remediation Workshop focuses on exploring use cases, requirements, technical challenges and lessons learned related to the use of security automation in enterprise remediation. The goal of the workshop is to actively engage the security automation community in developing open specifications that allow us to: identify and describe remediation actions, express remediation policies, assign tasks and report results of attempted corrective actions. The sessions in this track are focused on the technical aspects of security automation and are intended to be highly interactive.

Common Remediation Enumeration (CRE) and Extended Remediation Information (ERI) – Chris Johnson, NIST (moderator)

Christopher Johnson is a Computer Scientist at the National Institute of Standards and Technology (NIST) where he manages the National Vulnerability Database software flaw analysis activities, submissions to the National Checklist Program and hosting of Security Content Automation Protocol data sources. Prior to joining NIST, Mr. Johnson worked as consultant to Federal and State government agencies and the investment banking, securities and insurance industries. Mr. Johnson was a founder and principal of an information assurance practice that provided vulnerability assessment, security architecture design, code development, certification and accreditation, and security testing and evaluation services. His research interests include security automation, software flaw analysis, and security metrics.

Remediation Policy – Matthew Wojcik, MITRE (moderator)

Matthew Wojcik is a Lead Information Security Engineer at the MITRE Corporation. He has been involved with security standardization efforts at MITRE for the past ten years. Matt is currently project lead for CCE™, and member of a team developing proposed specifications for remediation standardization. He was the original moderator of the OVAL® Board, and is a past CVE® analyst and past member of MITRE's IDS team.

Remediation Tasking – Matthew Wojcik, MITRE (moderator)

Matthew Wojcik is a Lead Information Security Engineer at the MITRE Corporation. He has been involved with security standardization efforts at MITRE for the past ten years. Matt is currently project lead for CCE™, and member of a team developing proposed specifications for remediation standardization. He was the original moderator of the OVAL® Board, and is a past CVE® analyst and past member of MITRE's IDS team.

Remediation Language – Matt Kerr, G2 (moderator)

Matt has been a system administrator and software developer for the past 11 years, with a focus on security for the last 9. He helped develop the DISA Gold Disk and has been involved with SCAP since 2005.

Secstate: Integrating SCAP and Puppet for System Lockdown – Karl MacMillan, Tresys Technology

Karl MacMillan is the Vice President of Technology for Tresys Technology, author of "SELinux by Example: Using Security Enhanced Linux," and frequent speaker at virtualization, security and open source events nationwide. As a software developer, designer, and technical leader, Karl has delivered secure solutions in support of the most sensitive security missions, including those at defense and intelligence agencies, and created compelling open source and proprietary software and products. At Tresys he is responsible for developing and driving technical strategy and implementation across a diverse range of services and solutions.

SCAP Product Validation Workshop
Room 318/319

This workshop will discuss current status of the SCAP Validation Program as well as planned changes for the coming year. All are invited to attend, but it is of primary interest to vendors that plan to build SCAP functionality into their products and to laboratories conducting SCAP testing.

Program Summary

This session will address the current status of the SCAP Validation Program along with a description of it's design and purpose.

Derived Test Requirements from the SCAP Specification

This session will present how tests should be tied directly to requirements within the SCAP specification and discuss the benefits and challenges of doing so.

Looking Ahead

As the program continues to expand, new ways of testing products and administering validations becomes necessary. We will discuss several proposed actions with particular attention paid to the upcoming USGCB testing for Windows 7/IE8 and Red Hat Enterprise Linux 5.

Open Discussion

Continuous Monitoring Workshop
Ballroom II

Continuous security monitoring is a necessary capability for defending against today's advanced cyber threats. This workshop will begin with a talk on continuous monitoring (CM) technical foundations (definition, maturity model, enterprise architecture view, and technical architecture views) followed by an industry and government panel to discuss CM technical designs. In the rest of the workshop, the participants will break out into facilitated groups to discuss and solve issues with CM automation, standardization, and defining useful measures that provide visibility into the security posture of organizations. The primary focus and goal of the workshop is to generate useful quantitative metrics that organizations can use to monitor and defend their systems.

Foundations for CM – Peter Mell, Harold Booth, and Dave Waltermire, NIST

This session will take a deep dive into foundational elements to enable technical continuous security monitoring. It will start from a definition and then derive essential characteristics. It will then take an enterprise architecture view and drive down through technical architectures to necessary components, interfaces, and communication models. The session will end discussing needed requirements and validation programs to enable continuous monitoring implementations within government.

Peter Mell is a senior computer scientist in the Computer Security Division at the National Institute of Standards and Technology (NIST). He is currently researching continuous security monitoring and related security automation capabilities. His past work includes creating the U.S. National Vulnerability Database, co-founding the NIST Security Content Automation Protocol (SCAP), and creating the SCAP product validation program. He was also the lead author of the Common Vulnerability Scoring System (CVSS) vulnerability metric used to secure credit card systems worldwide and he initiated the Federal Risk and Authorization Management Program (FedRAMP) for enabling government-wide risk management of large outsourced and multi-agency systems. His research experience includes the areas of cloud computing, security metrics, security automation, vulnerability databases, and intrusion detection systems.

Harold Booth is a Computer Scientist at the National Institute of Standards and Technology (NIST). Harold leads the development team for the National Vulnerability Database (NVD) and is also heavily involved in the development of the Security Automation Program specifications.

David Waltermire is an IT Specialist at the National Institute of Standards and Technology (NIST). He is the specification architect for the Security Automation Program and has been a significant contributor to the Security Content Automation Protocol (SCAP) and other security automation efforts.

CM Technical Design Panel – Peter Mell, NIST (moderator), Kim Watson, NSA, Ron Gula, Tenable, Duncan Hays, IRS, Randy Barr, Qualys

This panel will discuss technical issues with implementing technical continuous security monitoring within government. The panelists will provide different but complementary perspectives (metrics and scoring aggregation, necessary vendor tools, and actual

government implementations) to assist listeners in implementing continuous monitoring programs.

This session will take a deep dive into foundational elements to enable technical continuous security monitoring. It will start from a definition and then derive essential characteristics. It will then take an enterprise architecture view and drive down through technical architectures to necessary components, interfaces, and communication models. The session will end discussing needed requirements and validation programs to enable continuous monitoring implementations within government.

Peter Mell is a senior computer scientist in the Computer Security Division at the National Institute of Standards and Technology (NIST). He is currently researching continuous security monitoring and related security automation capabilities. His past work includes creating the U.S. National Vulnerability Database, co-founding the NIST Security Content Automation Protocol (SCAP), and creating the SCAP product validation program. He was also the lead author of the Common Vulnerability Scoring System (CVSS) vulnerability metric used to secure credit card systems worldwide and he initiated the Federal Risk and Authorization Management Program (FedRAMP) for enabling government-wide risk management of large outsourced and multi-agency systems. His research experience includes the areas of cloud computing, security metrics, security automation, vulnerability databases, and intrusion detection systems.

Ms. Kim Watson is the Technical Director for Information Analysis Transformation in VAO. She has been at NSA for over 20 years, most of which has been spent in VAO or one of its predecessor organizations. For the last 6 years Ms. Watson has been performing analysis of network data, with a focus on how to represent and relate different aspects of the network security environment (e.g., vulnerability, threat, impact). Her goal is to help define the standards, models, and frameworks required to support and enable more accurate and actionable risk decisions.

Mr. Gula is known in the global security community as a visionary, innovator and engineer of extraordinary talent. He traces his passion for his work in security to starting his career in information security at the National Security Agency conducting penetration tests of government networks and performing advanced vulnerability research. Since co-founding Tenable in 2002, Mr. Gula has been CEO and CTO at Tenable, maker of the world-renowned Nessus Vulnerability Scanner and Unified Security Monitoring enterprise solution. As CEO/CTO of Tenable, he is responsible for product strategy, research and development, and product design and development. Mr. Gula is also a leader in his community and a passionate advocate for education and scientific research. Prior to Tenable, Mr. Gula was the original author of the Dragon IDS and CTO of Network Security Wizards which was acquired by Enterasys Networks.

Duncan Hays, CISSP, is a Project Manager within the IRS Cybersecurity IT Security Projects office. For the past three years he has been working on a project to deploy a SCAP validated solution to perform continuous monitoring. Through this project, the IRS has contributed content to the SCAP community including OVAL® definitions for Windows and UNIX server platforms and CCE™ dictionary. IRS is an active participant in the development of DHS' Continuous Asset Evaluation, Situational Awareness, and Risk Scoring (CAESARS) Reference Architecture. Prior to joining the IRS he spent ten years at the Peace Corps designing, securing and building web applications.

As Chief Security Officer (CSO) of Qualys, Randy is responsible for security, risk management and business continuity planning of the QualysGuard platform used by thousands of organizations worldwide. He will also lead the Qualys CSO Advisory Board efforts to collaborate with customers on forging and implementing security and compliance best practices. Randy has over 13 years of information technology and leadership experience. Prior to joining Qualys, he was the Information Security Officer at Yodlee responsible for insuring a high-level security posture of Yodlee's Internet based financial services. Before Yodlee, Randy served as CSO for WebEx Communications, a Cisco company; the leading provider of web communication services with over 30,000 customers worldwide. At WebEx, Randy built a security department from the ground up and was responsible for the company's global security infrastructure. In this role, he led the company's successful attainment of the SysTrust Seal, SAS-70 Type II incorporating the ISO-17799 Control Objectives. Randy held several management positions within WebEx and leadership positions in the healthcare, gaming and high-tech industries. Randy is a frequent speaker at security conferences including CSO Perspectives, RSA, BITS Security Forum, The Security Standard and SaaS/Gov. He has also been quoted in numerous articles and was featured on the front cover of SC Magazine. Randy holds a BS in Business Administration from University of Phoenix.

Identifying Continuous Monitoring Measures – David Waltermire, NIST, Matt Coose, DHS

The National Institute of Standards and Technology and the United States Department of Homeland Security are sponsoring a workshop "Deriving data via automated feeds from Security Tools to generate useful and actionable information for awareness and reporting". The purpose of the workshop is to generate dialog on automation, standardization and defining and generating useful measures that provide visibility into the security posture of organizations. The workshop is open to Government and private sector participants as well as the services and software vendor communities. The format of the workshop will be to hold breakout sessions and provide the opportunity for representatives from each breakout to report out on their discussions, findings and recommendations. Breakout sessions will focus on the following areas: software assurance, network-based security, host-based security, vulnerability analysis and management, authorization and access control, and security management tools.

Matt Coose is the Director of Federal Network Security (FNS) for the National Cyber Security Division of the Department of Homeland Security within the National Protection and Programs Directorate (NPPD). The FNS program works across the federal government to improve cybersecurity posture by monitoring and measuring capabilities, assessing gaps, influencing policy and

strategy, and driving implementation of risk mitigation efforts. He was recently appointed to a senior OMB Task Force to develop cybersecurity metrics to be reported by all Federal agencies starting in 2010. He also chairs the Federal Systems Security Governance Board (FSSGB), providing guidance to the Information Systems Security Line of Business (ISSLOB), a joint OMB and DHS strategic sourcing body for cybersecurity related acquisitions.

David Waltermire is an IT Specialist at the National Institute of Standards and Technology (NIST). He is the specification architect for the Security Automation Program and has been a significant contributor to the Security Content Automation Protocol (SCAP) and other security automation efforts.