7th Annual IT Security Automation Conference

October 31 – November 2, 2011 • Crystal City, Virginia
Hyatt Regency

Conference Agenda

Monday, October 31

7:00 – 8:30 am	**Registration and Breakfast** – Foyer	
8:30 – 10:15 am	**Opening Remarks: Donna Dodson, Chief, Computer Security Division/Deputy Cyber Security Advisor, NIST** **Welcome Address: Dr. Patrick Gallagher, Deputy Undersecretary for Standards and Technology, and Director of NIST** **Keynote Address: Tony Sager, Information Assurance Chief Operating Officer, NSA** **Plenary Session: Building Security Beneath the OS** – Steve Orrin (Intel), David O'Berry (McAfee) **Track Lead Address**	
10:15 – 10:45 am	**Break** – Vendor Expo Hall	
	CONTINUOUS MONITORING	**SOFTWARE ASSURANCE**
Room	Regency E&F	Potomac 3, 4, 5 & 6
10:45 – 11:30 am	**Panel: Paradigm Change – What do we need to do differently to succeed?** - George Moore (State), Kim Watson (NSA), Joe Wolfkiel (DISA), Tim McBride (DHS), Kelley Dempsey (NIST), Nadya Bartol (Booz Allen)	**Mitigating the Risk of Zero-Day Attacks with Software Security Automation** – Joe Jarzombek (DHS), Tom Millar (DHS), and John Banghart (NIST)
11:45 – 12:30 pm	**Maximizing ROI for Continuous Monitoring** – Nadya Bartol (Booz Allen), Jamie Miller (Booz Allen)	**Measure Software Security** – Sean Barnum (MITRE)
12:30 – 1:30 pm	**Lunch** – Vendor Expo Hall	
1:30 – 2:15 pm	**Boyd's OODA Loop and Continuous Monitoring** - Tim Keanini (nCircle)	**Cyber Observables eXpression (CybOX) - Use Cases** - Richard Struse (DHS) and Sean Barnum (MITRE)
2:30 – 3:15 pm	**Continuous Monitoring for Federal Information Systems** - Earnest Neal (ASG) and Steve Johnston (Tripwire)	**Workshop: Risk Analysis and Measurement with CWRAF** – Richard Struse (DHS) and Steve Christey (MITRE)
3:15 – 3:45 pm	**Break** – Vendor Expo Hall	
3:45 – 4:30 pm	**Continuous Monitoring 2.0: Creating a Federal Benchmark Community in the Cloud** - Keren W. Cummins (nCircle)	**Malware Attribute Enumeration and Characterization (MAEC)** - Penny Chase (MITRE) and Ivan Kirillov (MITRE)
4:45 – 5:30 pm	**Panel: Strategic View of Continuous Monitoring – The Vision and How to Get There** - Matt Coose (DHS), Peter Mell (NIST), Michele Iversen (Education), Michael Jones (US Army), Rick Hill (Booz Allen)	**Toward CWE Compatibility Effectiveness and CWE Coverage Claims Representation (CCR)** – Paul E. Black (NIST) and Richard Struse (DHS)
5:30 – 6:30 pm	**Reception –** Vendor Expo Hall and Foyer	

Tuesday, November 1

7:30 – 8:30 am	**Registration and Breakfast** – Foyer				
8:30 – 10:15 am	**Welcome Address** – Regency E&F **Plenary Session: Building a Continuous Monitoring Program at the Department of Justice with Security Automation** – Holly Ridgeway (DoJ) **Plenary Session: Intrusions and Incident Handling: The Big Problem** – Joseph Drissel (Cyber ESI) **Track Lead Address**				
10:15 – 10:45 am	**Break** – Vendor Expo Hall				
	CONTINUOUS MONITORING	**AUTOMATION SPECIFICATIONS**	**NETWORK AUTOMATION**	**IT SECURITY THREATS**	**VENDOR PRODUCT HIGHLIGHTS**
Room	Regency E&F	Potomac 3&4	Potomac 1&2	Potomac 5&6	Tidewater 2
10:45 – 11:30 am	**Gaps in Automated Situational Awareness** - Joe Wolfkiel (DISA)	**SCAP 1.2 Overview** - David Waltermire (NIST), Karen Scarfone (Scarfone Cybersecurity)	**Getting the Network Security Basics Right (Part 1)** - Paul Bartock (NSA), Steve Hanna (Juniper)	**The Future Landscape of IT Security Threats** - David O'Berry (McAfee)	**Cutting Through the SIEM/Log Management Vendor Marketing** – A. N. Ananth (Prism Microsystems)
11:45 – 12:30 pm	**Implementing Situational Awareness with Continuous Compliance in Federal Agencies** - Brandon Wood (IBM)	**Common Platform Enumeration (CPE) 2.3 Specification Suite Overview** - Brant Cheikes (MITRE)	**Getting the Network Security Basics Right (Part 2)** - Paul Bartock (NSA), Steve Hanna (Juniper)	**IT Security Insights: On the Frontline of the Threat Landscape** - Marc Maiffret (eEye Digital Security)	**Identifying & Sharing Threat Information with OpenIOC** - Douglas Wilson (Mandiant)
12:30 – 1:30 pm	**Lunch** – Vendor Expo Hall				
1:30 – 2:15 pm	**Continuous Monitoring Technical Reference Model Overview** - Peter Mell (NIST)	**NVD CPE Dictionary Management Practices** - Chris McCormick (Booz Allen)	**Automating Network Security Assessment (Part 1)** - Doug Dexter (Cisco)	**Anti-Phishing Working Group Adventures in Information Sharing: Now and for the Future** - Pat Cain (APWG)	**PowerShell Support in SCAP 1.2** - Michael Tan (Microsoft)
2:30 – 3:15 pm	**Panel: Continuous Monitoring Technical Reference Model** - Peter Mell (NIST), Kent Landfield (McAfee), Tim Keanini (nCircle), Kathleen Moriarty (EMC), Adam Montville (Tripwire)	**OVAL 5.10 Update** Jon Baker - (MITRE)	**Automating Network Security Assessment (Part 2)** - Doug Dexter (Cisco)	**The Evolution of Collective Intelligence** - Wes Young (REN-ISAC)	**Security Configuration Simplified with the Microsoft Security Compliance Manager (SCM)** - Vlad Pigin (Microsoft)
3:15 – 3:45 pm	**Break** – Vendor Expo Hall				
3:45 – 4:30 pm	**Emerging Trends in Automated Continuous Monitoring Operations Research** - Paul Suh (Booz Allen)	**XCCDF 1.2 Update** - Charles Schmidt (MITRE)	**Panel: Future of Security Compliance and Automation (Part 1)** - Paul Bartock (NSA), Steve Hanna (Juniper), Doug Dexter (Cisco), Kent	**IETF MILE, Improving Incident and Information Sharing Standards** - Kathleen Moriarty (EMC)	**Using Vanguard Configuration Manager for Continuous Monitoring of NIST Security Controls on the IBM z/OS Operating System**

			Landfield (McAfee), Matt Webster (Lumeta)		**Environment** - Brian Marshall (Vanguard Integrity Professionals)
4:45 – 5:30 pm	**800-137: Information Security Continuous Monitoring for Federal Information Systems and Organizations** - Kevin Stine (NIST) and Kelley Dempsey (NIST)	**A Trust Model for Security Automation Data** - Harold Booth (NIST)	**Panel: Future of Security Compliance and Automation (Part 2)** - Paul Bartock (NSA), Steve Hanna (Juniper), Doug Dexter (Cisco), Kent Landfield (McAfee), Matt Webster (Lumeta)	**Enabling Coordinated Incident Handling and Information Sharing** - Tom Millar (US-CERT), Marcos Osorno (JHU-APL), Paul Cichonski (NIST)	**Using OVAL for Information Security Application Integration** - Marlon Gaspar (Modulo)

Wednesday, November 2

7:30 – 8:30 am	**Registration and Coffee** – Foyer			
8:30 – 10:00 am	**Welcome Address** – Regency E&F **Plenary Presentation: Using OCIL to Improve Health Information Security** – John Paul Chalpin (Exeter Government Services), Matthew Smith (G2), Gunnar Engelbach (ThreatGuard) **Plenary Presentation: Cloud Computing Security for DoD / Governments (U.S.)** - Antonio Mauro **Track Lead Address**			
10:00 – 10:30 am	**Break**			
	CONTINUOUS MONITORING	**AUTOMATION SPECIFICATIONS**	**NETWORK AUTOMATION**	**FUTURE OF GLOBAL VULNERABILITY REPORTING**
Room	Regency E&F	Potomac 1&2	Potomac 3&4	Potomac 5&6
10:30 – 11:15 am	**Effective Measures for Continuous Monitoring** - Dr. George Moore (Dept. of State)	**Common Configuration Scoring System (CCSS)** - Karen Scarfone (Scarfone Cybersecurity)	**From Mobile Workers to IPv6 - How to Secure Today's Networks** - Randy Lee (Fortinet)	**Panel: The State of Global Vulnerability Reporting** – Tom Millar (US-CERT), Richard Struse (DHS), Steve Boyle (MITRE), Harold Booth (NIST), Art Manion (CERT/CC), Joe Hemmerlein (Microsoft)
11:30 – 12:15 pm	**New Requirements For Continuous Monitoring In The Cloud** – Matt Alderman (Qualys)	**ARF 1.1 and Asset Identification 1.1** - Adam Halbardier (Booz Allen)	**Security Coordination with IF-MAP** - Matt Webster (Lumeta)	**Panel: The Future of Global Vulnerability Reporting** – Tom Millar (US-CERT), Richard Struse (DHS), Art Manion (CERT/CC), Kent Landfield (McAfee), Tim Keanini (nCircle), Steve Boyle (MITRE)
12:15 – 1:15 pm	**Lunch** – On your own			
1:15 – 2:00 pm	**SP 800-53: The Common Link Between SCAP and Common Criteria** - Eric Winterton (Booz Allen)	**SCAP 1.2 Datastream Formats** - Adam Halbardier (Booz Allen)	**Security: A Coordinated Approach** - Stephen Hanna (Juniper)	**Workshop: Issues in Global Vulnerability Reporting and Identification** – Tom Millar (US-CERT), Richard Struse (DHS)
2:15 – 3:00 pm	**Enabling Enterprise Security Management Solution Interoperability Through SCAP** - Adam Schnitzer (Booz Allen)	**Asset-Based Summary Results Reporting** - Mark Davidson (MITRE)	**SCAP for Inter-Networking Devices** - Luis Nunez (C3i Security)	

3:00 – 3:30 pm	**Break**			
3:30 – 4:15 pm	**Operational Aspects of Continuous Monitoring** - Almaz Tekle (Deloitte & Touche), Christian Neeley (Deloitte & Touche)	**Tasking and Targeting of Assessments** - Adam Halbardier (Booz Allen)	**Content Repositories: Operational Approaches and Commercial Directions** – Kent Landfield (McAfee), Aharon Chernin (SCAP.com), Chandrashekhar Basavanna (Secpod)	**Efficiency in Security Audits - The Standards Journey of McAfee Policy Auditor** - Lal Narayanasamy (McAfee)
4:30 – 5:15 pm	**Providing Risk Metrics Using Security Automation, Protocols, and Standards** - James Park (NSA)	**Standardizing Event and Log Management with CEE and EMAP** - George Saylor (G2), William Heinbockel (MITRE)	**Compliance Management for Mobile Devices** - Steve Tomasko (Booz Allen)	**Workshop: Implementing a Standards-Based Security Automation Program Outside of the Federal Government** - Aharon Chernin (SCAP.com)

7th Annual IT Security Automation Conference

October 31 – November 2, 2011 • Crystal City, Virginia
Hyatt Regency

Plenary Speakers & Sessions

Donna Dodson, Chief, Computer Security Division/Deputy Cyber Security Advisor, NIST
Ms. Dodson is the Division Chief of the Computer Security Division and Deputy Cyber Security Advisor at the National Institute of Standards and Technology (NIST). Ms. Dodson oversees NIST's cyber security program to conduct research, development and outreach necessary to provide standards, guidelines, tools, metrics and practices to protect the information and communication infrastructure. Under her leadership, the division collaborates with industry, academia and other government agencies in research areas such as security management and assurance, cryptography and systems security, identity management, security automation, secure system and component configuration, test validation and measurement of security properties of products and systems, security awareness and outreach and emerging security technologies. In addition, the division plays a role in both national and international security standards setting.

She recently received the Federal 100 Award and has been awarded the U.S. Department of Commerce's Gold and Bronze Medal Awards.

Patrick D. Gallagher, Deputy Undersecretary for Standards and Technology, and Director of NIST
Dr. Patrick Gallagher was confirmed as the 14th Director of the U.S. Department of Commerce's National Institute of Standards and Technology (NIST) on November 5, 2009. He also serves as Under Secretary of Commerce for Standards and Technology, a new position created in the America COMPETES Reauthorization Act of 2010, signed by President Obama on January 4, 2011.

Gallagher provides high-level oversight and direction for NIST. The agency promotes U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology. NIST's FY 2010 resources include $856.6 million from the Consolidated Appropriations Act of 2010 (Public Law 111-117), $49.9 million in service fees, and $101.5 million from other agencies. The agency employs about 2,900 scientists, engineers, technicians, support staff, and administrative personnel at two main locations in Gaithersburg, Md., and Boulder, Co.

Gallagher had served as Deputy Director since 2008. Prior to that, he served for four years as Director of the NIST Center for Neutron Research (NCNR), a national user facility for neutron scattering on the NIST Gaithersburg campus. The NCNR provides a broad range of neutron diffraction and spectroscopy capability with thermal and cold neutron beams and is presently the nation's most used facility of this type. Gallagher received his Ph.D. in Physics at the University of Pittsburgh in 1991. His research interests include neutron and X-ray instrumentation and studies of soft condensed matter systems such as liquids, polymers, and gels. In 2000, Gallagher was a NIST agency representative at the National Science and Technology Council (NSTC). He has been active in the area of U.S. policy for scientific user facilities and was chair of the Interagency Working Group on neutron and light source facilities under the Office of Science and Technology Policy. Currently, he serves as co-chair of the Standards Subcommittee under

the White House National Science and Technology Council.

Tony Sager, Chief Operating Officer for the Information Assurance Directorate, National Security Agency
Tony Sager is the Chief Operating Officer for the Information Assurance Directorate (IAD) at the National Security Agency. IAD's vision is to be the decisive defensive advantage enabling America and its allies to outmaneuver network adversaries. 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.

Building Security Beneath the OS – Steve Orrin (Intel), David O'Berry (McAfee)
This is a technical plenary address by individuals who own responsibility for secure systems with the technical vision and operational aspects of hardware and firmware's role in the creation of a secure stack. This address will provide the basis for hardware and firmware building blocks beneath the OS and why hardware and firmware matter in their position in the security stack.

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/Web Service 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 and Officer of WASC (Web Application Security Consortium) and a Co-Founder of the SafeSOA Taskforce. In 2009, Steve was named a fellow at the Center for Advanced Defense Studies.

Mr. O'Berry is a "reformed CxO/CIO currently working for 'The Dark Side' as a Strategic Systems Engineer for McAfee." He spent 19 years on the enterprise side as a network manager, Director of Information Technology Systems and Services and, most recently, Director of Strategic Development and Information Technology in the public sector. During that timeframe he was an advocate for standards-based networks and security, working with groups like Trusted Computing Group and The Open Group to further those causes. Active within the industry, he currently holds CISSP-ISSAP, ISSMP, CISSLP, CRMP, among other certifications including old school certs like Master Certified Novell Engineer (a fact he tries not to mention very often). He calls himself a professional mutt because his background and experiences have been anything but a planned path throughout his career. Most recently he was honored as a ComputerWorld Top 100 IT Leader for 2011, a fact he attributes to the amazing team that surrounded him during his service in the public sector.

Building a Continuous Monitoring Program at the Department of Justice with Security Automation – Holly Ridgeway (DoJ)

Over the past two years, the Department of Justice (DOJ) has deployed an automated endpoint management solution to serve as the foundation of their continuous monitoring program. The solution provides near-real time analysis of endpoint assets, including the status of patches, known vulnerabilities, configuration baseline compliance, and known anti-malware definitions. This talk will cover the solution rollout and lessons learned. It will address the development of a dashboard to help management better understand the Department's security posture and areas that may require additional focus. It will also consider future enhancements to the solution to address network and other devices.

Mrs. Ridgeway currently serves as the Department of Justice Deputy Chief Information Security Officer and Program Manager of the Justice Security Operations Center. Mrs. Ridgeway promotes collaboration and creativity to achieve DOJ's goals and objectives. In 2010, Mrs. Ridgeway received the prestigious Federal 100 award that recognizes individuals in government and industry who have made significant contributions to the federal information technology community. Also in 2010, she received the Justice Management Division Performance Award for successfully defending the Department during incidents and for the implementation of advanced capabilities in the Justice Security Operations Center.

Mrs. Ridgeway currently serves as an Adjunct Professor at the University Of Maryland, University College in the fields of Cybersecurity, Information Systems Management and Information Assurance. Mrs. Ridgeway earned a Bachelor of Science degree in Information Systems Management and a Master of Science in Computer Systems Management with a specialty in Information Assurance. She holds two certifications, Project Management Professional (PMP) and Certified Information System Security Professional (CISSP).

Intrusions and Incident Handling: The Big Problem – Joseph Drissel (CyberESI)
This presentation discusses the intrusion related challenges facing the nation and network defenses as a whole. The speed with which the adversary attacks and engages requires a new way of doing business. The presentation walks you through an entire Advanced Persistent Threat (APT) related attack and uncovers where the gaps are and where we must make adjustments. The discussion will cover specifics about what is working and what is not working.

Joseph Drissel is the Founder and CEO of CyberESI. CyberESI provides incident response, intrusion/malware analysis, training and cyber related intelligence to its clients and the community at large. Before founding CyberESI, Joseph was the Acting Section

Chief of the Intrusions Section at the Defense Computer Forensics Laboratory (DCFL). In this capacity Joseph and his team provided intrusion and malware analysis support to DoD entities, Federal Law Enforcement and the Defense Industrial Base.

Using OCIL to Improve Health Information Security – John Paul Chalpin (Exeter Government Services), Matthew Smith (G2), Gunnar Engelbach (ThreatGuard)

The NIST HIPAA Security Rule Self Assessment Toolkit, a self-contained, standalone, platform independent software application, helps organizations better understand the requirements of the HIPAA Security Rule, implement those requirements, and assess those implementations in their operational environment. This session will provide an overview of the NIST HIPAA Security Rule toolkit, and will describe how the Open Checklist Interactive Language (OCIL) specification is used within the context of this healthcare information security use case.

Mr. Chalpin is the Director of Engineering and Program Manager for NIST and HHS at Exeter Government Services in Gaithersburg, MD. Chalpin has a diverse background with emphasis in software engineering and Health IT initiatives and has led multiple technology teams. Chalpin has over 15 years of experience in project and technical management, has successfully guided organizations through their CMMI Level 2 and 3 assessments, and has served as Project Manager for large and complex development contracts. Chalpin holds a B.S. Degree in Biology and Premedical Studies from the College of Holy Cross in Worcester, MA, and is published, having supported research at the University of Massachusetts Medical Center. Chalpin received his Project Manager Professional certification in 2009.

Mr. Smith from G2 received his BS in Systems and Information Engineering in May 2009 from the University of Virginia where he founded and served as the first President of the NExT club, a group devoted to promoting awareness of interdisciplinary technologies and opportunities for R&D among the student body. Matthew went on to design software system architectures for submersibles, and now, as a software engineer for G2, he spearheads their technical efforts on the HIPAA security rule project and the use of social media for business.

Cloud Computing Security for DoD / Governments (U.S.) – Antonio Mauro (Independent Consultant)
This plenary session will provide a description of the U.S. approach for moving the Government and DoD applications and data into the Cloud. A description of the technology will first be provided (essential characteristics, service model, deployment model, etc.) followed by a description of the Federal Cloud Computing strategy and challenges, risks and opportunities and a brief summary of Federal and Defense Cloud initiatives and use cases.

Antonio Mauro, a Security Solutions Architect, has studied in the U.S.A. and he achieved a doctorate in Computer Engineering and Philosophy Doctor (PhD) in Electronic Communications and Cybercrime Security Governance, particular case: Military Defense and Public Safety and Security focus on U.S. Cloud Computing in Government and DoD. With ten years of experience in information technology and security solutions, Antonio currently works in the information security area for a major international company as a Security Solutions Architect designing and planning security architectures for important Government and Military organizations. He is a teacher in Networking, VoIP, Security, Computer Forensics and Digital Investigations in many Italian Universities. Antonio has co-authored several books on Information Security and Intelligence, Computer Forensics, Digital Investigations and Cloud Computing in U.S. Government. Antonio is also a member of numerous national and international professional associations. He also serves as a member (judge consultant) of the Court of Justice in Roma and is often appointed as an expert on computer forensics and digital investigations. Antonio has received appreciation letters for professionalism, expertise and excellent work from the Italian Air Force, Italian Navy, Italian Army, and Arma dei Carabinieri (Military Police).

7th Annual IT Security Automation Conference

October 31 – November 2, 2011 • Crystal City, Virginia
Hyatt Regency

Continuous Monitoring Track
Regency E&F

The concept and practice of continuous monitoring has blossomed into the keystone of federal information security programs. Continuous monitoring covers management, operational, and technical aspects of an information system program providing a comprehensive and holistic means to effectively manage these programs. Many security programs face challenges implementing and managing an effective information security program. The IT Security Automation Conference Continuous Monitoring track will offer a wide range of topics over three days of sessions that delve into the many facets of continuous monitoring. Information security programs across the federal government continue to struggle to successfully implement continuous monitoring, and this track will offer management techniques and strategies, policies and procedures, automated technical solutions, and provide various means to implement continuous monitoring with checks and balances. This track will give you tools, lessons, and strategies to improve your continuous monitoring program.

Panel: Paradigm Change – What do we need to do differently to succeed? - George Moore (State), Kim Watson (NSA), Joe Wolfkiel (DISA), Tim McBride (DHS), Kelley Dempsey (NIST), Nadya Bartol (Booz Allen)

Continuous Monitoring builds on a mature structure of Federal standards, guidelines, and practices. It also requires fundamental change in how we have done security for the last 10 years and creation of brand new practices and techniques. Unlearning of the old way of assessing security, figuring out effective ways of measuring security, architecting multiple tools in a way that they can produce a common operating picture and situational awareness, and creating frameworks and practices for how to put it together, are all key questions that need to be answered. The panel will address the latest concepts for measurement, near-real-time monitoring, using a variety of tools and data sources, and the emerging practices for continuous monitoring.

Dr. 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), and led the formation of information system management programs 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.

Ms. Watson is a Technical Director in the Analysis and Data Fusion Group, Fusion, Analysis, and Mitigations (FAM) Deputy Directorate, Information Assurance Directorate at the National Security Agency. She has been at NSA for almost 25 years, most of which has been spent in the Fusion, Analysis, and Mitigations Deputy Directorate or one of its predecessor organizations (i.e., some type of vulnerability discovery or technology evaluation activity). For the last 8 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., configuration, 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. Ms. Watson recently received the Exceptional Civilian Service Award and a Fed100 Award for her work in this area. Ms. Watson has a degree in Mathematics from Michigan State University and a very healthy obsession with the Detroit Red Wings.

Mr. Wolfkiel is the Defense Information Systems Agency Engineering Group Lead for the Computer Network Defense (CND) Enclave Security Division. He is responsible for engineering the DoD Security Configuration Management (SCM) initiative, which includes Continuous Monitoring capabilities. He retired from the US Air Force (AF) in 2010 as a Lieutenant Colonel. Prior to retirement, he was the Chief of the CND Research and Technology Program Management Office. While there, he developed standards for CND operational reporting and oversaw research into automated sharing of detected network activities along with inventory and compliance reporting to support continuous monitoring. Previous jobs include planning and budgeting for DoD enterprise CND at US Space Command and US Strategic Command as a staff officer serving as the Information Assurance Architect at the AF Communications Agency.

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).

Ms. Dempsey began her career in IT in 1986 as an electronics technician repairing PCs and printers before moving on to system administration and network management in the early 90s. While with the Department of the Navy in 1999, she began focusing on information system security by training for and then conducting a large scale DITSCAP certification and accreditation from start to finish. In 2001, Kelley joined the NIST operational Information Security team, managing the NIST information system certification and accreditation program through September 2008. Kelley joined the NIST Computer Security Division FISMA team in October 2008 and has co-authored NIST SP 800-128 (Security-Focused Configuration Management) and NIST SP 800-137 (Information Security Continuous Monitoring) and was also a major contributor to NIST SPs 800-53 Rev 3, 800-37 Rev 1, 800-53A Rev 1, and 800-39. Kelley completed a B.S. degree in Management of Technical Operations from Embry-Riddle Aeronautical University, graduating cum laude in December 2003 and earned a CISSP certification in June 2004.

Ms. Bartol advises numerous Federal agencies on the subjects of cyber security measurement, continuous monitoring, and cyber supply chain risk management and led numerous strategic groundbreaking cyber security engagements that included building brand new cybersecurity programs. She built a consecutive series of service offerings focusing in those areas rooted in national and international standards. Ms. Bartol co-authored several NIST special publications and interagency reports, including 800-55 Revision 1, Performance Measurement Guide for Information Security and NIST Interagency Report 7622, Piloting Supply Chain Risk Management Practices for Federal Information Systems. She serves as Co-chair of DoD/DHS/NIST SwA Measurement Working Group and in that capacity served as a principal author of Practical Measurement Guidance for Software Assurance and Information Security. Nadya led the development of Information Assurance Technology Analysis Center (IATAC) State of the Art Report, Measuring Cyber Security and Information Assurance. Nadya serves as United States delegate to an ISO committee dedicated to the development of cyber security standards where she is US technical expert working on the ISO/IEC 27000 series standards, Information Security Management System and a US Head of Delegation (HOD) for Working Group 1. She is a Project Editor for ISO/IEC 27036 – Information technology – IT security techniques – Information Security for Supplier Relationships.

Maximizing ROI for Continuous Monitoring – Nadya Bartol (Booz Allen), Jamie Miller (Booz Allen)

Continuous monitoring is becoming a requirement, as evidenced by NIST's mandate for "near-real time risk management" of information systems. The significant resources currently being spent on IT system re-certification must instead be directed toward continuous monitoring, enabling organizations to meet this requirement, while maximizing return on investment. This presentation will explore several techniques developed by the State Department and the National Security Agency to achieve maximum efficiency and effectiveness in testing security controls as part of a continuous monitoring program. We will specifically take a close look at the following concepts and how they can be used to maximize the return on investment for an organization's security value chain: Expected value of security based on risk, cost, and mean time to failure; Foundational and capability security controls; Effectiveness measures; Security event-driven testing; and Continuous monitoring lessons learned at the Department of State.

Ms. Bartol advises numerous Federal agencies on the subjects of cyber security measurement, continuous monitoring, and cyber supply chain risk management and led numerous strategic groundbreaking cyber security engagements that included building brand new cybersecurity programs. She built a consecutive series of service offerings focusing in those areas rooted in national and international standards. Ms. Bartol co-authored several NIST special publications and interagency reports, including 800-55 Revision 1, Performance Measurement Guide for Information Security and NIST Interagency Report 7622, Piloting Supply Chain Risk Management Practices for Federal Information Systems. She serves as Co-chair of DoD/DHS/NIST SwA Measurement Working Group and in that capacity served as a principal author of Practical Measurement Guidance for Software Assurance and Information Security. Nadya led the development of Information Assurance Technology Analysis Center (IATAC) State of the Art Report, Measuring Cyber Security and Information Assurance. Nadya serves as United States delegate to an ISO committee dedicated to the development of cyber security standards where she is US technical expert working on the ISO/IEC 27000 series standards, Information Security Management System and a US Head of Delegation (HOD) for Working Group 1. She is a Project Editor for ISO/IEC 27036 – Information technology – IT security techniques – Information Security for Supplier Relationships.

Mr. Miller is a Senior Associate at Booz Allen Hamilton Inc. where he serves as an information security governance and continuous monitoring thought leader and subject matter expert. Mr. Miller has assisted an international government, numerous commercial companies, and several U.S. Federal government Departments and agencies with standing up their information security and continuous monitoring programs – most notably helping the Department of State stand up their lauded continuous monitoring capability. Additionally, Mr. Miller helped stand-up the Booz Allen Cyber Security Program Diagnostic service offering that has been implemented by a number of Fortune 500 companies, as well as for an international government. Mr. Miller and his team are currently supporting a number of government clients that also include the Department of State, Department of Veterans Affairs, the World Bank Group, and the Office of Personnel Management. Mr. Miller is also a certified Project Management Professional and a Certified Functional Continuity Planner, and recently authored "Effective Information Security Governance: How to Address Enterprise-shared Risk", published in Security Magazine. Mr. Miller received his B.S. degree in International Studies from American University and possesses an M.B.A. in International Management from Thunderbird, School of Global Management.

Boyd's OODA Loop and Continuous Monitoring – Tim Keanini (nCircle)

Col. John Boyd (1927 - 1997) was a fighter pilot but is best known for his contribution to military strategy with the concept of the OODA loop. This concept has been used in business and in military strategy but recently many have been trying to apply this concept to IT security. The Continuous Monitoring initiative is essentially the observation and orientation (OO) steps of the OODA loop, but it is equally important that we understand how these steps drive decision and action (DA) within an organization. Applications of the OODA loop to date are flawed because IT security has no offensive measure. This talk will introduce everyone to the details of the OODA loop with an example of both right and wrong implementations. This talk will also address how continuous monitoring and automation can assist organizations applying the OODA loop by speeding up the decision cycles of the organization.

Mr. Keanini brings 20 years of technical expertise from both the information security and gaming industries, which provides him with unique insight into the dynamic problems customers face for risk management. As CTO, Tim's technical vision for nCircle has been shaped by his intimate understanding of both the "gaming mindset" which always takes into account an active opponent and his experience and respect for the ever-changing and complex nature of each customer's IT operations.

Continuous Monitoring for Federal Information Systems - Earnest Neal (ASG) and Steve Johnston (Tripwire)

This session will cover Continuous Monitoring (CM). ASG and Tripwire will demonstrate real world products following 800-37, 800-137 and CAESARS. Explanation of the Risk Management Framework (RMF) process. The track will demonstrate a system that currently has an ATO using the RMF process and explain how to put that system into CM process. Expand on the concept of grouping raw data feeds to create subsystems for the purpose of POA&M creation, tracking and closure. The CM solution will show how the creation of subsystems utilizing IT infrastructure data will create a holistic view of the enterprise down to the control level.

Mr. Neal has 15 years of experience, 13 of which were directly in the Information Security industry. He is an experienced consultant with proven capabilities and strong information security and system solutions project management capabilities. Mr. Neal is a SME of the FISMA process, control assessment, and process automation. Mr. Neal has spoken at numerous conferences about the RMF methodology, as well as this past year's 6th Annual IT Security Automation Conference. Neal specializes in the development of annual business planning, staffing, project delivery, and customer satisfaction. Before joining ASG, Mr. Neal was a member of the e-Security and ISS X-Force Professional Security Services team. While at Internet Security Systems, Mr. Neal planned and managed many network Intrusion Detection System (IDS) implementations on large enterprise networks to include fine tuning the network and host-based intrusion detection policies. Mr. Neal was a key decision maker at DoS with their current IDS deployment. Mr. Neal has also performed more than 65 vulnerability/penetration assessments for corporate and Government customers. Mr. Neal has assessed and reviewed new security technologies for customers, clarifying the pros and cons of each as they apply to the customer's environment.

Mr. Johnston, Federal Partner & Engineering Manager with Tripwire, Inc. has been seen as a trusted advisor and thought leader for information security and compliance within the federal government and financial industry for the past 12 years. Within his current position he works with cyber security partners and System Integrators on best of breed solutions to thwart against the evolving threat vector. Consulting and permanent positions held over the past years include Principal Consultant / business development for a leading MSP focused on the financial industry, Regional Engagement Manager and various contracted InfoSec and ITIL projects. In these roles, Steve has acted as an auditor, developer and provider of security solutions including hands-on experience with security operations, penetration testing and audit preparation. Most recently Steve's focus has been on security automation (SCAP) and the recently updated NIST Risk Management Framework requirements around continuous monitoring. Steve has presented many of these topics at SANS, InfoWeek Government and Government Executive.

Continuous Monitoring 2.0: Creating a Federal Benchmark Community in the Cloud - Keren W. Cummins (nCircle)

Continuous Monitoring 2.0 will rely on the concept of a cloud-based federal benchmark community that will play a significant role in helping agencies evaluate existing security investments and gauge the success of their programs. What will it take to make this concept a reality for the federal community?

This session will discuss the future of crowdsourcing government security metrics, the potential of leveraging cloud technologies to provide visual scorecards and benchmark comparisons, and how industry is currently using a benchmark community to improve their security infrastructure and share information.

Ms. Cummins is Director, Federal Markets for nCircle where she works with government agencies to provide tools for large-scale enterprises, in the arenas of agentless asset discovery and profiling, configuration compliance management, change auditing, and file integrity monitoring. Previously, Cummins was VP Public Sector for Phoenix Technologies where she worked with federal agencies and partners on device authentication and other BIOS-level services. Cummins also held the position of VP Government Services for Digital Signature Trust. Before joining the commercial sector, Cummins worked for the Commerce Department and served on the Federal Public Key Infrastructure Steering Committee (FPKI SC).

Panel: Strategic View of Continuous Monitoring – The Vision and How to Get There - Matt Coose (DHS), Peter Mell (NIST) , Michele Iversen (Education), Michael Jones (US Army), Richard Hill (Booz Allen)

Federal Community is rapidly moving towards implementing Continuous Monitoring capabilities. A regulatory requirement, Continuous Monitoring is a way to gain near-real-time insights into security posture, reduce paperwork, and save costs. Critical strides have been made towards putting in place government-wide capabilities and infrastructure to make this happen. Leading agencies are implementing the practices and creating the first series of lessons learned. The panel will address strategic lessons learned from early implementation and the vision for what is coming in the near future.

Mr. 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.

Mr. 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. Iversen is the Director of Information Assurance (IA) and Chief Information Security Officer for the Department of Education leading a highly skilled team of Information Assurance and Cyber Security professionals in the protection and defense of the Department's networks, financial systems, and sensitive privacy information. Prior to joining the Department of Education, Ms. Iversen spent more than twenty-two years in the Department of Defense and the Intelligence Community where she served as the Chief of Information System Security Engineering for the National Security Agency and as the DOD Computer Network Defense (CND) Architect under the Assistant Secretary of Defense for Identity and Information Assurance where she oversaw and provided guidance on DOD Computer Network Defense policy, architecture and data Strategies, Computer Emergency Response Teams, and IA and CND Education, Training, and Awareness. Ms. Iversen has also served as a Global Network Vulnerability Analyst in both the Intelligence and DoD Communities. She served twelve years on active duty as a Signal Officer in the United States Army where in addition to a diverse background in strategic and tactical communications systems she participated in the establishment of the Joint Task Force for Computer Network Defense a precursor organization of US Cyber Command. Ms. Iversen is an Army Reserve Officer who completed a tour in Southwest Asia as the Chief of the Regional Computer Emergency Response Team –Southwest Agency in 2008.

Mr. Jones is the Chief of Emerging Technologies for the CIO/G6 Cyber Directorate. He is a retired U.S. Army officer with over 27 years of service where he worked in the IT field since 1995. He operated the Army National Guard's worldwide network (GuardNet) for four years, and has served as an IT Plans and Policy Chief; Deputy Director of the Enterprise Technology Service Activity, Director of the Office of Information Assurance and Compliance and as the Deputy Director for the Army Cyber Task Force. He holds the Information Technology Infrastructure Library (ITIL) foundation certification, is a Lean Six Sigma green belt; completed the Chief Information Officer (CIO) course with Information Assurance (IA) emphasis from the National Defense University and successfully completed the Certified Information Security Manager (CISM) test. 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.

Mr. Hill, a Principal at Booz Allen Hamilton has more than 28 years of consulting experience in information systems, information security and information infrastructure. Rick is responsible for leading a broad portfolio of cybersecurity programs at NIST, the Department of State, Agriculture, GSA and several other Federal agencies. Mr. Hill (PMP) holds Bachelors in Electrical Engineering and a M.B.A. from Johns Hopkins University.

Gaps in Automated Situational Awareness - Joe Wolfkiel (DISA)

This presentation will provide an overview of data collection, reporting, correlation, and business logic required to build a continuous monitoring capability for the DoD that meets Certification and Accreditation (C&A) and Cyber Readiness Situational Awareness (SA) requirements. Mr. Wolfkiel will provide an overview of the DoD's N-Tiered reporting structure, the sensor data required, and the challenges that will need to be addressed.

Mr. Wolfkiel is the Defense Information Systems Agency Engineering Group Lead for the Computer Network Defense (CND) Enclave Security Division. He is responsible for engineering the DoD Security Configuration Management (SCM) initiative, which includes Continuous Monitoring capabilities. He retired from the US Air Force (AF) in 2010 as a Lieutenant Colonel. Prior to retirement, he was the Chief of the CND Research and Technology Program Management Office. While there, he developed standards for CND operational reporting and oversaw research into automated sharing of detected network activities along with inventory and compliance reporting to support continuous monitoring. Previous jobs include planning and budgeting for DoD

enterprise CND at US Space Command and US Strategic Command as a staff officer serving as the Information Assurance Architect at the AF Communications Agency.

Implementing Situational Awareness with Continuous Compliance in Federal Agencies - Brandon Wood (IBM)

When it comes to systems and security management, organizations struggle to balance the resources spent for security with the resources needed to measure and report against the myriad of regulations such as FDCC, HIPAA, and agency mandates. Space and time is the enemy, and existing processes and tools aren't up to the challenge. The gap is only increasing and the results often catastrophic. Clearly, more help is needed within organizations to assist with these challenges, enable continuous compliance, and achieve situational awareness throughout the infrastructure.

Please join us to learn how you can achieve situational awareness and continuous compliance by gaining comprehensive visibility into the security posture of assets throughout the infrastructure - physical or virtual, on and off the network – and gain the following benefits:

- Centralized real-time visibility into the current state of all managed computing assets
- Continuous host-based assessment and enforcement of security policies with minimal system impact
- Proven reduction of endpoint configuration and update cycle from days and weeks to minutes and hours
- Closed loop reconciliation of policy remediation and enforcement
- Ability to manage roaming devices from a central location

Mr. Wood is the Public Sector, Manager of Technical Sales for Tivoli Endpoint Manager at IBM. Mr. Wood brings 10 years of experience in systems and security management, including his previous role as Deputy Branch Chief of End User Technology at the Securities Exchange Commission. He has worked with a large number of government organizations, designing and implementing cutting edge technologies to meet and exceed continuous monitoring and Government security mandates.

Continuous Monitoring Technical Reference Model Overview (Presentation and Panel) – Peter Mell (NIST), Kent Landfield (McAfee), Tim Keanini (nCircle), Kathleen Moriarty (EMC), Adam Montville (Tripwire)

This session will discuss the continuous monitoring reference model jointly developed by the NSA, DHS, and NIST. The goal is to enable federated, interoperable continuous monitoring implementations that support both operations and compliance. Data aggregation and analysis among tiered instances is key, as well as management of digital policy, and orchestration and tasking of diverse security tools. This session will present an overview of the model and the results of a nine week industry and government review. It will end with an industry panel discussing the benefits, challenges, and Federal government usage of the model.

Mr. 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.

Mr. Landfield has spent 25+ years in software development, global network operations and network security arenas. He is currently 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 the catalyst in McAfee adopting SCAP component standards across three different security technologies. 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 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 IETF 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 other emerging standards working groups.

Mr. Keanini brings 20 years of technical expertise from both the information security and gaming industries, which provides him with unique insight into the dynamic problems customers face for risk management. As CTO, Tim's technical vision for nCircle has been shaped by his intimate understanding of both the "gaming mindset" which always takes into account an active opponent and his experience and respect for the ever-changing and complex nature of each customer's IT operations.

Ms. Moriarty is with the EMC Office of the CTO working on technology strategy and standards for Governance, Risk, and Compliance with a focus on incident response and related areas. Kathleen has been the primary author of multiple published standards and actively contributes to security standards activity in both the ITU-T and the IETF. Previously, as the practice manager for security consulting at EMC, Kathleen was responsible for oversight of key projects, and development of security programs, in

addition to serving as the acting CISO of a global investment banking firm. Kathleen has also been the head of IT Security at MIT Lincoln Laboratory and the Director of Information Security at FactSet Research Systems. Kathleen holds a Masters of Science degree in Computer Science from Rensselaer Polytechnic Institute and a Bachelor of Science in Mathematics and Computer Science from Siena College.

Mr. Montville, as the Security and Compliance Architect for Tripwire, Inc. leads a team of researchers and architects providing the company with security and compliance domain expertise. From humble beginnings as a secure hash implementer at Oregon State University's Information Security Laboratory in the mid '90s, Mr. Montville has come to be a voice in the Security Automation and larger security community. Mr. Montville has held a variety of security-related positions throughout his fourteen year information security career, including civil service at the Department of Defense, CTO of a secure messaging company, and Director of IT Operations for a secure information sharing service. He is an avid blogger on information security topics, and believes that being a hacker is not equivalent to being evil.

Emerging Trends in Automated Continuous Monitoring Operations Research - Paul Suh (Booz Allen)

Considering the growth and complexity of Information Technology systems in society as well as the push for automated continuous monitoring in the Federal government, there is a need to understand (1) the types of commercial tools available, (2) the operational characteristics of available tools, and (3) the business benefits of implementing a stronger automated continuous monitoring program. Unfortunately, how to develop an automated continuous monitoring program is hampered by the myriad of IT security tools in the marketplace, by each organization's underlying IT infrastructure and IT security program maturity, as well as by growing budget constraints. The presenter would like to share the latest trends in the Automated Continuous Monitoring Operations in the areas of (1) comparing IT security infrastructure tools, (2) recommending minimum automated continuous monitoring tool and operational characteristics, as well as (3) a model for justifying the investment in these new technologies. In addition, we would like to provide a high-level overview of the latest Cyber Security Tool resources by the Department of Defense and Information System Security Line of Business resources for the Federal community, great places for anyone interested in Continuous Monitoring tools to start.

Mr. Suh develops Federal IT Security solutions at the Booz Allen Hamilton Cyber Technology Center of Excellence. He focuses on security architecture and government efficiency in support of several Federal Agencies, including NIST, DHS, IRS, VA, DoD, and CMS. He is a Certified Information Systems Security Professional as well as a graduate of the University of North Carolina at Chapel Hill and North Carolina State University.

NIST SP 800-137: Information Security Continuous Monitoring for Federal Information Systems and Organizations - Kevin Stine (NIST) and Kelley Dempsey (NIST)

Information security is a dynamic process that must be effectively and pro-actively managed to be able to identify and respond to new vulnerabilities, evolving threats, and an organization's constantly changing enterprise architecture and operational environment. Continuous monitoring, a critical part of an organization's risk management process, helps to ensure that organization-wide operations remain within an acceptable level of risk, despite the changes that occur.

This session will discuss NIST Special Publication 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations. The purpose of this guideline is to assist organizations in the development of a continuous monitoring strategy and the implementation of a continuous monitoring program providing visibility into organizational assets, awareness of threats and vulnerabilities, and visibility into the effectiveness of deployed security controls. It provides ongoing assurance that planned and implemented security controls are aligned with organizational risk tolerance as well as the information needed to respond to risk in a timely manner.

Mr. Stine is an Information Security Specialist in the Security Management and Assurance Group within the National Institute of Standards and Technology's (NIST) Computer Security Division. At NIST, he focuses on applying information security standards, practices, and technologies to the Health Information Technology sector, publishing information security standards and guidelines; conducting outreach and awareness, and advancing security performance measurement. Kevin also serves as the chairperson of the Federal Computer Security Managers' Forum, an informal group sponsored by NIST to promote the sharing of information system security information among federal agencies.

Ms. Dempsey began her career in IT in 1986 as an electronics technician repairing PCs and printers before moving on to system administration and network management in the early 90s. While with the Department of the Navy in 1999, she began focusing on information system security by training for and then conducting a large scale DITSCAP certification and accreditation from start to finish. In 2001, Kelley joined the NIST operational Information Security team, managing the NIST information system certification and accreditation program through September 2008. Kelley joined the NIST Computer Security Division FISMA team in October 2008 and has co-authored NIST SP 800-128 (Security-Focused Configuration Management) and NIST SP 800-137 (Information Security Continuous Monitoring) and was also a major contributor to NIST SPs 800-53 Rev 3, 800-37 Rev 1, 800-53A Rev 1, and 800-39. Kelley completed a B.S. degree in Management of Technical Operations from Embry-Riddle Aeronautical University, graduating cum laude in December 2003 and earned a CISSP certification in June 2004.

Effective Measures for Continuous Monitoring and Assessment - Dr. George Moore (Dept. of State)

Federal agencies must follow NIST SP 800-53 to test up to a thousand detailed aspects of “controls” to validate that security programs are working. This presentation shows how fourteen “effectiveness measures” a) can “cover” testing all the 800-53 controls, b) allow measurement of whether the security program is blocking attacks, c) guide root cause analysis and remediation when effectiveness lags, and d) allow for effective and efficient continuous assessment and authorization of information systems.

Dr. 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.

New Requirements For Continuous Monitoring In The Cloud – Matt Alderman (Qualys)

Cloud computing poses new challenges for IT security, compliance, and audit professionals who must protect agency data and IT assets, and verify compliance of security controls. The cloud uproots predictability of traditional IT architectures, security controls, and audit procedures, and forces cloud service subscribers to cede two vital capabilities to cloud service providers: (1) control of data, programs, and actions and (2) visibility on status of data and program usage.

Mr. Alderman is Director of Product Management for Qualys and is responsible for product direction of Qualys’ compliance offerings. Matt has over 20 years of experience in information security and compliance, which includes over 10 years developing and managing comprehensive programs that address risk and compliance. His focus has been on developing applications to automate risk and compliance requirements. Prior to joining Qualys, Matt was founder and CTO of ControlPath, a GRC software solution that was acquired by TrustWave in 2008. While at ControlPath, Matt and co-inventor Sean Molloy were issued United States Patent 7,788,150: Method for assessing risk in a business.

SP 800-53: The Common Link Between SCAP and Common Criteria - Eric Winterton (BAH)

Since the adoption of NIST SP 800-53 by both the Security Content Automation Protocol (SCAP) and Common Criteria (CC) little attention had been paid to the fact that there is a link between both. Not all security features evaluated by the Common Criteria are automated responses to threats nor are the security controls identified in NIST SP 800-53. But as more networks and digital assets come online (e.g., laptops, tablets, and mobile devices) the need to automate as many prevention, detection, and reaction security mechanisms as possible is needed by administration professionals. Network and system administrators need to manage configurations of more devices while eliminating and detecting vulnerabilities of those devices. Meanwhile, budgets for administration are not growing at the same pace as the technology introduced.

This presentation will show the linkage between SCAP, NIST SP 800-53, and the Common Criteria. To deliver SCAP compliant security controls that are CC validated, we will show how Common Criteria can leverage SCAP capabilities and implement security controls identified in the NIST SP 800-53.

Mr. Winterton, CISSP, is the Director of the Booz Allen Hamilton Common Criteria Laboratory. He has over 20 years of direct experience in information assurance systems, security engineering, and security product testing. Mr. Winterton has been performing IA product assessments for the past 12 years and he holds an undergraduate degree in computer science and a Master's Degree from Johns Hopkins University.

Enabling Enterprise Security Management Solution Interoperability Through SCAP - Adam Schnitzer (Booz Allen)

Enterprise Security Management (ESM) provides the foundation for ensuring the trust and integrity of enterprise information and allows flexible and fine-grained control of information sharing. ESM comprises the systems and resources required to order, create, disseminate, modify, suspend and terminate management controls to provision and operate Information Assurance services, processes and devices across the enterprise. ESM requires organizational assets to reference authoritative sources of record to provide subject and attribute information.

The primary purpose of ESM is to enforce the protection of critical assets that reside within an organization. Therefore, an ESM solution (“the/an ESM”) must have the ability to identify these critical assets and define policies which govern how they are handled. Today many of these products are point solutions with lack of interoperability. SCAP allows for a standard way to query configuration of remote endpoints in an enterprise. This paper will show how SCAP can help standardize communications across the enterprise, and make recommendations for where these solutions need to evolve to meet bigger demands.

Mr. Schnitzer, PMP is a Lead Associate within Booz Allen Hamilton's Cyber Technologies Center of Excellence. He currently leads numerous efforts supporting the development of enterprise security strategy, policy, and architecture for the Department of Defense. Throughout his career he served as a Surface Warfare Officer in the U.S. Navy; an instructor at the U.S. Naval Academy; a Command, Control, Communications and Intelligence (C4I) systems engineer; and an information security professional. Mr.

Schnitzer has an undergraduate degree in Systems Engineering from the U.S. Naval Academy and a graduate degree in National Security and Strategic Studies from the U.S. Naval War College. He is a Project Management Professional (PMP) and holds a CompTIA Security+ certification.

Operational Aspects of Continuous Monitoring - Almaz Tekle (Deloitte & Touche), Christian Neeley (Deloitte & Touche)

Understanding the relationship between IT risk, security program design and effective continuous monitoring methodologies allows agencies to envision CM strategies that not only meet individual programmatic requirements, but rally the organization's people, processes and technology in their work toward a common IT security goal. In this session, we discuss a common risk-focused framework and nomenclature, founded on the principles set forth by NIST, that empowers agencies to consistently identify their risks, frame their impacts throughout the mission, and effectively leverage their existing people and technology resources as they move toward operationalizing a continuous monitoring program. As the foundation for this framework, we will discuss the importance of understanding the scope of the transformation and defining an end-state and formulating a Continuous Monitoring Transition Strategy that aligns with the organization's strategic goals and budget constraints.

Ms. Tekle CISSP, CISM, CISA, is a principal at Deloitte & Touche, LLP. She has more than 22 years of experience serving Federal clients in civilian and defense agencies supporting information risk management and privacy projects. In her current role, she leads cross federal solution development and project support for security program management, risk and compliance management, and cyber security architecture development. Ms. Tekle received her B.S. degree in Computer Science from the University of DC and received her M.S. degree in Technical Management from Johns Hopkins University.

Mr. Neeley is a Senior Manager with Deloitte & Touche, LLP. He has over 11 years of experience supporting a variety of clients within the federal government and commercial sectors, developing IT Risk Management and Continuous Monitoring programs, building NIST-based technical assessment solutions and deploying Security Architecture review boards in the SDLC. He currently leads Deloitte's internal IT Risk Management solution offering development and deployment, designing the firm approach to Continuous Monitoring in the public sector. He holds a BA degree from the University of Virginia in Finance and Economics.

Providing Risk Metrics Using Security Automation, Protocols, and Standards - James Park (NSA)

In an applied research initiative to establish SCAP in a continuous monitoring application, the National Security Agency's Computer Network Defense Research and Technology Team developed a reference implementation of a standards-based, extensible risk scoring engine as part of an integrated security auditing system. This session describes the findings, and previously unknown, unanticipated, or unforeseen gaps in the process and technology necessary to support an enterprise-wide, standards-based, tool agnostic information system risk awareness capability.

Mr. Park is a Computer Network Defense Research and Technology (CND R&T) project manager at NSA Information Assurance Directorate. Mr. Park has a diverse background from being an engineer on nuclear powered submarines, to information technology systems engineer, to Computer Network Operations (CNO) planner while in active duty Navy. Since retirement from the Navy, Mr. Park has been focusing on research activities supporting network security continuous monitoring.

Software Assurance Track

Potomac 3, 4, 5 & 6

It is estimated that 90 percent of reported security incidents result from exploits against defects in the design or implementation of software. Vulnerabilities in software can jeopardize intellectual property, consumer trust, and business operations and services. Additionally, a broad spectrum of critical applications and infrastructure, from process control systems to commercial application products, depend on secure, reliable software. In order to ensure system reliability, integrity, and safety, it is critical to address security throughout the software lifecycle.

The presentations in this track will explore software assurance techniques and tools to quantify and fundamentally improve the security and reliability of systems. Attendees will gain insights into practical techniques that they can use today to enhance the security and reliability of the software that they build or deploy. In addition, the speakers will demonstrate how organizations can use processes and tools to set priorities and make practical risk-based security decisions.

Mitigating the Risk of Zero-Day Attacks with Software Security Automation – Joe Jarzombek (DHS), Tom Millar (DHS), and John Banghart (NIST)

For the Nation's critical infrastructure to be reliable, resilient, robust, and secure, the software supporting it must also have the same qualities. A broad spectrum of critical applications and infrastructure, from process control systems to commercial application products, depend on secure, reliable software. It is estimated that 90 percent of reported security incidents result from exploits against defects in the design or build of software. Therefore, ensuring the integrity and resiliency of software is vital to protecting the infrastructure from threats which target software vulnerabilities, and reducing overall risk from cyber-attacks. In order to ensure system reliability, integrity, and safety, it is critical to include provisions for built-in security of the enabling software.

Mr. 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).

Mr. Millar joined US-CERT in 2007 as a network analyst. Since then he has served as a senior watch officer, deputy operations manager, and chief of communications, playing a significant role in coordination and response to activities during major cyber events such as the 2007 Estonian DDoS attacks, Conficker's countdown, the US DDoS attacks of 2009 and several others. He holds an M.S. in Engineering Management and Systems Engineering from George Washington University.

Mr. Banghart has 15 years in the IT/IS industry, having spent several years in the private sector building and operating Internet services, followed by several years at the Center for Internet Security, where he led groups of security experts in the development of over 20 security checklists. His work in security automation and SCAP dates back nearly 10 years, and he has been an active participant in the development of several SCAP specifications. He is currently the Security Automation Program Manager at the National Institute of Standards and Technology, where he oversees the National Vulnerability Database, the National Checklist Program, the SCAP Validation Program, and the ongoing development and international standardization of security automation specifications.

Measure Software Security – Sean Barnum (MITRE)

Until recently, the absence of a common measure for software weaknesses has limited the software industry's ability to assess and remediate exploitable software flaws. The Common Weakness Enumeration (CWE) is a key initiative sponsored by DHS NCSD SwA program with additional funds from the Department of Defense (primarily through the National Security Agency). CWE represents a joint effort of the US Federal Government and the software stakeholder community with MITRE providing technical leadership and project coordination. CWE is a standardized dictionary used in diagnosing exploitable software faults and reporting findings, enabling interoperability among tools and automation of risk mitigation measures. Over 840 software weaknesses have been identified and catalogued, and 49 software diagnostic tools and services offer CWE-compatible capabilities. Learn how CWE helps organizations assess and remediate exploitable software flaws.

Mr. 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 23 years of experience in the software industry in the areas of development, software quality assurance, quality management, process architecture & improvement, knowledge management and security.

Cyber Observables eXpression (CybOX) - Use Cases - Richard Struse (DHS) and Sean Barnum (MITRE)

Exchange of meaningful information among cybersecurity data sources is a critical step on the path to effective automated defense against modern threats. How can we refine the open specifications so that event data and observable indicators may be parsed, filtered, and correlated by diverse families of cybersecurity systems in concert? What are the ways these standards could be leveraged by the community to better share automated network defense strategies? Attendees will be given a demonstration of a CybOX use case.

Mr. Struse is the Deputy Director for Software Assurance in the Department of Homeland Security's National Cyber Security Division where he oversees efforts relating to the automation of Software Assurance. Prior to joining DHS, Mr. Struse was Vice President of Research and Development at VOXEM, Inc., where he was responsible for the architecture, design and development of a high-performance, extremely high-reliability communications software platform that is in use in telecommunications systems around the world. He began his technical career at Bell Laboratories where his work focused on tools to automate software development and the UNIX operating system.

Mr. 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 23 years of experience in the software industry in the areas of development, software quality assurance, quality management, process architecture & improvement, knowledge management and security.

Risk Analysis and Measurement with CWRAF – Richard Struse (DHS) and Steve Christey (MITRE)

To better enable software stakeholders to reduce risks attributable to the most significant exploitable software errors relevant to specific business/mission domains and technologies, the DHS NCSD SwA program has sponsored the development of the Common Weakness Risk Analysis Framework (CWRAF) that uses the Common Weakness Scoring System (CWSS) scoring criteria with CWE to provide consistent measures for prioritizing risk mitigation efforts and focusing secure coding practices, enabling better informed decision-making for the development and acquisition of more resilient software products and services.

CWRAF enables more targeted specification of "Top-N" CWE lists that are relevant to specified technologies used within specific business domains. In the past, the Top 25 CWE lists have represented community collaboration efforts to prioritize the most exploitable constructs that make software vulnerable to attack or failure. Now, with CWRAF business domains can use the scoring criteria with CWE to identify exploitable software fault patterns that are most significant to them in specific technologies: web applications, control systems, embedded systems, end-point computing devices, operating systems, databases, storage systems, enterprise system applications, and cloud computing services. In this workshop, participants will construct one or more CWRAF "vignettes" for specific business domains.

Mr. Struse is the Deputy Director for Software Assurance in the Department of Homeland Security's National Cyber Security Division where he oversees efforts relating to the automation of Software Assurance. Prior to joining DHS, Mr. Struse was Vice President of Research and Development at VOXEM, Inc., where he was responsible for the architecture, design and development of a high-performance, extremely high-reliability communications software platform that is in use in telecommunications systems around the world. He began his technical career at Bell Laboratories where his work focused on tools to automate software development and the UNIX operating system.

Mr. Christey is a Lead INFOSEC Engineer in the Security and Information Operations Division at The MITRE Corporation. After joining MITRE in 1989, he initially conducted research in artificial intelligence (AI), moving into the information security arena in 1993. He was the primary security auditor for MITRE's networks from 1994 to 1999, conducting network-based risk assessment, management, and incident response. Since 1997, he has conducted research which blends his experience in AI and security, in topics such as automated vulnerability analysis of source code, reverse engineering of executable code, and distributed security assessment. From 1999 to the present, he has been the editor of the Common Vulnerabilities and Exposures (CVE) list, and the Chair of the CVE Editorial Board. Mr. Christey holds a B.S. in Computer Science from Hobart College.

Malware Attribute Enumeration and Characterization (MAEC) - Penny Chase (MITRE) and Ivan Kirillov (MITRE)

The balance between secure development and secure operations can be provided with help from Malware Attribute Enumeration and Characterization (MAEC), Common Attack Pattern Enumeration and Classification (CAPEC), and the Cyber Observables.

Ms. 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 M.A. in History of Science and an M.S. in Computer Science from Harvard University.

Mr. Kirillov is the technical lead behind the MAEC effort and the primary author of the MAEC schemas. He has been working in the information security realm at MITRE after graduating with an M.S. in Computer Science from Georgia Tech in 2009. Besides data modeling and malware research, his interests lie in web app programming and the non-security related but fascinating field of robotics.

Toward CWE Compatibility Effectiveness and CWE Coverage Claims Representation (CCR) – Paul E. Black (NIST) and Richard Struse (DHS)

The Common Weakness Enumeration (CWE) defines a unified, measurable set of software weaknesses that is enabling more effective discussion, description, selection, and use of software security tools and services that detect weaknesses in software. To encourage and recognize use of CWEs, MITRE has established the CWE Compatibility and Effectiveness Program. Phases 1 and 2 of the program establish that tool warnings accurately map to CWEs. Phase 3 establishes which CWEs a tool (or capability) can identify and locate via testing. In this session, we propose (1) ideas on what constitutes acceptable fundamental and broad test sets for Phase 3, and (2) that the SAMATE Reference Dataset (SRD) be the repository and access for such test sets.

The CCR is a lightweight schema that allows a software analysis tool and/or service provider to state claims as to those CWEs that their technology or process can discover. This session is targeted to tool/service vendors and tool/service consumers with the goal of refining the CCR model for public release. Issues to be addressed include the specificity of claims, “anti-claims,” and key use-cases for CCR.

Mr. Black has nearly 20 years of experience in software for IC design, software quality assurance, and business data processing. For a decade he has been a Computer Scientist in the Information Technology Laboratory at NIST. Black has published in the areas of software testing and configuration control, queuing analysis, formal methods, software verification, quantum computing, and computer forensics.

Mr. Struse is the Deputy Director for Software Assurance in the Department of Homeland Security’s National Cyber Security Division where he oversees efforts relating to the automation of Software Assurance. Prior to joining DHS, Mr. Struse was Vice President of Research and Development at VOXEM, Inc., where he was responsible for the architecture, design and development of a high-performance, extremely high-reliability communications software platform that is in use in telecommunications systems around the world. He began his technical career at Bell Laboratories where his work focused on tools to automate software development and the UNIX operating system.

Automation Specifications Track
Potomac 3&4

The typical IT enterprise today utilizes a variety of products to support IT security and operations. Integrating these capabilities to support organizational needs is often a resource intensive and challenging endeavor. Many current solutions do not integrate and interoperate well, creating barriers to collecting, aggregating and analyzing operational information to support organizational decision making. The specifications track will address new and revised specification activities and standardization efforts that are targeted to reduce existing and future barriers, enabling greater interoperability in the IT enterprise.

SCAP 1.2 Overview - David Waltermire (NIST), Karen Scarfone (Scarfone Cybersecurity)

This session will cover an overview of SCAP 1.2 as documented in SP 800-126 Rev 2. It will focus on the changes since the previous revision, including the addition of OVAL 5.10, XCCDF 1.2, CPE 2.3, Trust Model for Security Automation Data (TMSAD), and a source and results data stream format, among other things.

Mr. 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.

Ms. Scarfone is the Principal Consultant for Scarfone Cybersecurity. She provides cybersecurity publication consulting services to Federal agencies, specializing in security automation standards and network and system security guidelines. Karen was formerly a Senior Computer Scientist for the National Institute of Standards and Technology (NIST), and she has co-authored over 50 NIST Special Publications and Interagency Reports, including more than 15 related to security automation. She holds bachelor's and master's degrees in computer science and she has 20 years of professional experience in the IT field. Karen's security domains include general security engineering and administration, wired and wireless network security, host security, incident response, intrusion detection, log management, vulnerability measurement, and security automation.

Common Platform Enumeration (CPE) 2.3 Specification Suite Overview – Brant Cheikes (MITRE)

High level overview of the suite of specifications that make up CPE 2.3, including information about the state of CPE 2.3 and where it is today, where we are headed as consumers of CPE 2.3.

Mr. Cheikes is a Principal Scientist at the MITRE Corporation. He currently directs the CPE project at MITRE, orchestrated the work of the CPE Core Team that resulted in the recent publication of four NIST Interagency Reports comprising the CPE 2.3 specification suite, and was the primary author of the CPE 2.3 Naming Specification. Brant holds a Bachelor's degree in Computer Engineering from Boston University, and M.S. and Ph.D. degrees in Computer and Information Science from the University of Pennsylvania.

NVD CPE Dictionary Management Practices - Chris McCormick (Booz Allen)

A follow-on presentation and discussion to the Common Platform Enumeration (CPE) 2.3 Specification Suite Overview regarding CPE management at the National Vulnerability Database (NVD).

Mr. McCormick is a cybersecurity professional working for Booz Allen Hamilton. He supports the National Institute of Standards and Technology (NIST) Security Automation Program. Specifically, Mr. McCormick serves as the senior vulnerability analyst for the National Vulnerability Database (NVD), the lead analyst for the National Checklist Program (NCP), as well as the Common Platform Enumeration (CPE) Official Dictionary moderator. Mr. McCormick has over ten years of information technology experience with a concentration in Information Assurance and Cybersecurity in the last three years. Mr. McCormick currently holds the EC Council Certified Ethical Hacker (CEH) and CompTIA Security+ certifications.

OVAL 5.10 Update – Jon Baker (MITRE)

The current state of the Open Vulnerability and Assessment Language (OVAL) will be discussed. Topics will include an overview of the major changes in OVAL Version 5.10 which will be included in SCAP 1.2 as well as the most notable changes to the OVAL Language since SCAP 1.1. This session will also briefly discuss some of the future plans for OVAL and encourage participants to get involved in the OVAL community to help shape the direction of this open community effort.

Mr. Baker is a Principal Information Security Engineer at the MITRE Corporation. He currently leads the OVAL team at MITRE and has spent the past eight 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 Bachelor's degree in Psychology from Tufts University and a Master's degree in Computer Science from Boston University.

XCCDF 1.2 Update – Charles Schmidt (MITRE)

The recently released XCCDF 1.2 contains a number of new features and changes relative to XCCDF 1.1.4. This talk will provide an overview of the changes, guidelines for updating XCCDF 1.1.4 content to use the new schema, and walk-throughs of the use of some of the more significant changes, such as the new Tailoring element and complex-values.

Mr. Schmidt is a Lead Information Security Engineer at the MITRE Corporation. He has supported security guidance development efforts for more than 11 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. Charles holds a Bachelor's degree in both Mathematics and Computer Science from Carleton College and a Master's degree in Computer Science from the University of Utah.

A Trust Model for Security Automation Data – Harold Booth (NIST)

NIST IR 7802 establishes recommendations for establishing a trust model for security automation content. This session will review some of the use cases the model was designed to address and will provide a technical overview of the trust model.

Mr. 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 a contributor to the development of the Security Automation Program specifications.

Common Configuration Scoring System (CCSS) – Karen Scarfone (Scarfone Cybersecurity)

The Common Configuration Scoring System (CCSS) is a measurement and scoring system for the severity of software security configuration issues. Although CCSS is derived from the Common Vulnerability Scoring System (CVSS), it has significant differences. In this session, we will discuss the basics of CCSS, explain how CCSS and CVSS differ, and clear up misconceptions regarding how CCSS can and should be used.

Ms. Scarfone is the Principal Consultant for Scarfone Cybersecurity. She provides cybersecurity publication consulting services to Federal agencies, specializing in security automation standards and network and system security guidelines. Karen was formerly a Senior Computer Scientist for the National Institute of Standards and Technology (NIST), and she has co-authored over 50 NIST Special Publications and Interagency Reports, including more than 15 related to security automation. She holds bachelor's and master's degrees in computer science and she has 20 years of professional experience in the IT field. Karen's security domains include general security engineering and administration, wired and wireless network security, host security, incident response, intrusion detection, log management, vulnerability measurement, and security automation.

ARF 1.1 and Asset Identification 1.1 – Adam Halbardier (Booz Allen)

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 included in NIST Special Publication (SP) 800-126 - Security Content Automation Protocol (SCAP) Rev 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 emphasis on introducing the audience to these emerging specifications and their role in the larger security automation landscape.

Mr. 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 is coauthor of NIST Special Publication 800-126 - The Technical Specification for the Security Content Automation Protocol (SCAP): SCAP Version 1.2, NIST Interagency Report (IR) 7802 - Trust Model for Security Automation Data 1.0, NIST IR 7693 - Asset Identification 1.1, and NIST IR 7694 - Asset Reporting Format 1.1. He also maintains the SCAP Content Validation Tool. Mr. Halbardier has a Bachelor's Degree in Computer and Electrical Engineering from the University of California, Irvine.

SCAP 1.2 Datastream Formats – Adam Halbardier (Booz Allen)

As part of SCAP 1.2, source and result data stream formats have been defined for SCAP content. This session will cover the reasoning and motivation behind the introduction and design of these formats, as well as a technical overview of them.

Mr. 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 is coauthor of NIST Special Publication 800-126 - The Technical Specification for the Security Content Automation Protocol (SCAP): SCAP Version 1.2, NIST Interagency Report (IR) 7802 - Trust Model for Security Automation Data 1.0, NIST IR 7693 - Asset Identification 1.1, and NIST IR 7694 - Asset Reporting Format 1.1. He also maintains the SCAP Content Validation Tool. Mr. Halbardier has a Bachelor's Degree in Computer and Electrical Engineering from the University of California, Irvine.

Asset-Based Summary Results Reporting – Mark Davidson (MITRE)

The Asset Summary Reporting Format (ASR) is a data model to express the transport format of summary information about one or more sets of assets. The standardized data model facilitates the interchange of aggregate asset information throughout and between organizations. ASR is vendor and technology neutral, flexible, and suited for a wide variety of reporting applications.

Mr. Davidson is an Information Security Engineer at The MITRE Corporation. Mark is currently working on the Asset Reporting specifications in conjunction with NIST and a variety public sector companies. Mark works with SCAP standards in his other work at MITRE. Mark has a background in Information Security, having previously performed the Information Security Analyst role for a Security Operations Center in a Fortune 100 Financial company. Mark has a BS in Computer Science from UMass Amherst.

Tasking and Targeting of Assessments – Adam Halbardier (Booz Allen)

This session will cover initial ideas and requirements for a common tasking and targeting language that will help enable the collection of assessments across an enterprise in a consistent and standards-based manner. It will focus on presenting the concept, requirements, approach, and initial high-level model.

Mr. 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 is coauthor of NIST Special Publication 800-126 - The Technical Specification for the Security Content Automation Protocol (SCAP): SCAP Version 1.2, NIST Interagency Report (IR) 7802 - Trust Model for Security Automation Data 1.0, NIST IR 7693 - Asset Identification 1.1, and NIST IR 7694 - Asset Reporting Format 1.1. He also maintains the SCAP Content Validation Tool. Mr. Halbardier has a Bachelor's Degree in Computer and Electrical Engineering from the University of California, Irvine.

Standardizing Event and Log Management with CEE and EMAP – George Saylor (G2), William Heinbockel (MITRE)

Common Event Expression (CEE) is a core piece of the NIST Event Management Automation Protocol (EMAP). With the first public release of MITRE's CEE event standard (August 2011), this presentation introduces the audience to the CEE v0.6 architecture and specifications, including overview and examples of each component of CEE. This presentation will also introduce proposed components of the EMAP suite of specifications; these specifications will assist in standardizing event parsing and event correlation rules. The presentation will be given in an open discussion format that allows audience members to participate and provide input into the future direction of CEE and EMAP.

Mr. 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.

Mr. Heinbockel is the creator and lead for Common Event Expression, CEE, for The MITRE Corporation. Over the past few years, he has worked closely with both public and private organizations to gather requirements and improve situational awareness (SA) and enterprise security management (ESM) through better event logs. William received his Bachelors and Masters degrees in Computer Science from the Rochester Institute of Technology.

Network Automation Track
Potomac 1&2

Just imagine what your IT team can do if they had a few extra hours each day, if you could relieve them of some of the many reactive and manual tasks. Network security continues to be mostly a manual process, worsened by the difficulties in gathering coherent information about users, devices and activities on the network. More than ever, the system administrators running our networks are at the crossroads of justifying their time between providing quality of service to the users, or maintaining a level of mandated compliance with a plethora of reporting tasks which often do not translate to quality of service nor to improved security. 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. In addition, users are continually pushing the envelope in devices that connect to the enterprise LAN, in the form of mobile devices such as iPads, netbooks, wireless access points (WAPs) and, of course, mainstay laptops and PCs that everyone uses every day. The ability to grasp the "big picture" continues to be absent. The Network Automation track will address new and proven assessment capabilities, open standards initiatives aimed at automating integration of network security systems.

Getting the Network Security Basics Right (Parts 1 and 2) - Paul Bartock (NSA), Steve Hanna (Juniper)

Network security is a complex art, with many variations depending on the requirements of the network owner and users. However, there are some basics that everyone must consider: access control, management, intrusion detection, incident handling, etc. In this talk, we'll examine several typical customer scenarios and the approaches that may be taken to address them. Special emphasis will be placed on using open architectures and standards to assure maximum flexibility.

Mr. Bartock is the Technical Director for The Mitigations Group for The Fusion, Analysis and Mitigation (FAM) Associate Directorate in the Information Assurance Directorate at NSA. He is responsible for working with DoD, federal government, and private industry stakeholders to promote the use of security standards and best practices to protect DoD and federal computer networks. He partners with the leading operating system vendors to encourage participation in government standards activities. For past 13 years, he provided technical guidance on the government consensus work groups to influence the development of the security baseline configurations, which led to the OMB-mandated Federal Desktop Core Configuration (FDCC) and the US Gov't Configuration Baselines (USGCB). Drawing on his extensive knowledge of networks, he developed and published countermeasure guidance to mitigate vulnerabilities in DoD and US Gov't networks. Mr. Bartock is a graduate of the University of Maryland and is a Certified Information Systems Security Professional and a Network Certified Engineer. In 2008, he received the Exceptional Civilian Service Award and Federal 100 Award for his work developing the federal security baselines. In 2009, he was elevated to the Senior Executive Service (SES).

Mr. 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.

Automating Network Security Assessment (Parts 1 & 2) - Doug Dexter (Cisco Systems, Inc.)

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.

Mr. 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.

Panel: Future of Security Compliance and Automation (Parts 1 & 2) - Paul Bartock (NSA), Steve Hanna (Juniper), Doug Dexter (Cisco), Kent Landfield (McAfee), Matt Webster (Lumeta)

In a world where we the good guys, they the bad guys, and everyone in between all use the same technology, all are interconnected, and we all use the one in the same market place, it's difficult to stay ahead. In this panel session, industry leaders and shakers will exchange latest industry initiatives, paradigm shifts necessary and visions for the future on how to stay ahead of the game in

providing a level of automated service with reliable security in this hostile and dynamic cyberspace.

Mr. Bartock is the Technical Director for The Mitigations Group for The Fusion, Analysis and Mitigation (FAM) Associate Directorate in the Information Assurance Directorate at NSA. He is responsible for working with DoD, federal government, and private industry stakeholders to promote the use of security standards and best practices to protect DoD and federal computer networks. He partners with the leading operating system vendors to encourage participation in government standards activities. For past 13 years, he provided technical guidance on the government consensus work groups to influence the development of the security baseline configurations, which led to the OMB-mandated Federal Desktop Core Configuration (FDCC) and the US Gov't Configuration Baselines (USGCB). Drawing on his extensive knowledge of networks, he developed and published countermeasure guidance to mitigate vulnerabilities in DoD and US Gov't networks. Mr. Bartock is a graduate of the University of Maryland and is a Certified Information Systems Security Professional and a Network Certified Engineer. In 2008, he received the Exceptional Civilian Service Award and Federal 100 Award for his work developing the federal security baselines. In 2009, he was elevated to the Senior Executive Service (SES).

Mr. 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.

Mr. 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.

Mr. Landfield has spent 25+ years in software development, global network operations and network security arenas. He is currently 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 the catalyst in McAfee adopting SCAP component standards across three different security technologies. 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 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 IETF 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 other emerging standards working groups.

Mr. 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 as Client Services Manager for BankOne (Chase).

From Mobile Workers to IPv6 - How to Secure Today's Networks - Randy Lee (Fortinet)

Today's threats are no longer focused on single device elements; device exploits are multi vector in nature and becoming more intelligent every day. Offensive and defensive security systems have complex challenges that are constantly changing, making the task to stay on top of current security threats more difficult. How to address these complex challenges will be covered and discussed.

Mr. Lee, an infrastructure systems veteran with 19+ years of engineering experience, is currently a Director of Federal Engineering Services at network security vendor Fortinet, Inc. Prior to Fortinet, Randy was the Infrastructure Manager for Foundry Networks, leveraging strong information systems and development experience to deliver robust enterprise class architecture and services. Before Foundry, Randy was a Technical Account Manager for Mainsoft where his responsibilities included helping customers port their Windows applications to Unix/Linux platforms. Randy also held senior engineering positions at Covasoft, IBM/Tivoli and Applied Materials. He recently presented at several conferences and trade shows on the topic of evolving threat prevention.

Security Coordination with IF-MAP - Matt Webster (Lumeta)

This session will explore how implementing network security automation, from the mostly manual process that exists in most large enterprises and government networks today, will enable organizations to keep pace with the changing cyber security threat landscape. This session will also focus on how network security automation can help drive down the cost of network security

management.

Mr. Webster has over 20 years of 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 as Client Services Manager for BankOne (Chase).

Security: A Coordinated Approach - Stephen Hanna (Juniper)

Today's security environment is composed of isolated independent systems, unable to share information in a structured and actionable way. A VPN gateway authenticates the user and checks endpoint health but cannot pass this information to or receive an alarm from an IDS. New open standards enable such information sharing, thus addressing complex attacks and reducing costs.

Mr. 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.

SCAP for Inter-Networking Devices – Luis Nunez (C3ISecurity)

Survey on SCAP for inter-networking devices such as routers and switches. The critical infrastructure and enterprise networks today are built on routers and switches to transport communications to endpoints and beyond. SCAP expansion into discovering and interrogating inter-networking devices fits into this continuous monitoring paradigm. The presentation will cover traditional SCAP methods used to probe devices and will discuss other methods. The presentation will also explore current and future SCAP capabilities for inter-networking devices.

Mr. Nunez is an Information Assurance consultant with C3i Security, an Information security consulting practice based out of RTP North Carolina. For the last 5 years Luis has been working in the area of Information Assurance in the US Federal sector focusing on SCAP and related standards. Luis is familiar with the DoD IA process and is intimately familiar with DISA STIGs. Luis' expertise stems from his military experience along with his civilian work with security consulting firms.

Content Repositories: Operational Approaches and Commercial Directions – Kent Landfield (McAfee), Aharon Chernin (SCAP.com), Chandrashekhar Basavanna (Secpod)

After creating the capability for using standardized content for policy, device hardening and state evaluations, we are faced with a distribution problem. This presentation will address the issues and operational approaches in the future as well as discuss the emerging approaches and attitudes toward providing commercial repository capabilities. This presentation will also provide a view and demo of two commercial content repositories and how they are seen fitting into the future.

Mr. Landfield has spent 25+ years in software development, global network operations and network security arenas. He is currently 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 the catalyst in McAfee adopting SCAP component standards across three different security technologies. 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 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 IETF 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 other emerging standards working groups.

Mr. Chernin has over 15 years of IT experience. He has worn many hats during this time including: Unix Systems Manager, Web Application Developer, Vice President of Storage Deployment at JPMorgan, and now as a Security Automation Program Manager in the financial sector. He uses these diverse experiences to come up with unique solutions to real world security industry problems. Aharon is a standards and automation fanatic and an expert in vulnerability management. As such he built one of the first entirely automated and standards based vulnerability management programs in the private sector. Aharon also sits on the board for the OVAL standard. He is also one of the top contributors of vulnerability content to the MITRE OVAL repository with over 2,000 definition submissions. Aharon sees a future where all of information security is standards based, automated, and objective.

Mr. Basavanna is the Founder and CEO of SecPod Technologies. SecPod is uniquely positioned as a security content provider, operating in all aspects of Security Management. He's responsible for setting and executing the strategy and vision for the company, along with managing the day to day operations of the company. He has been an active member of OpenVAS, an open source vulnerability scanner, providing the technology direction for the project and also a member of the OVAL board. He was instrumental in launching the first commercial, subscription based OVAL definitions feed. Under his leadership, SecPod has released a number of

security advisories along with contributing to the open source community projects.

Compliance Management for Mobile Devices - Steve Tomasko (Booz Allen)

The capabilities and use of mobile devices (smartphones, tablets, etc) has grown exponentially in recent years. Most DoD Services and Agencies are interested in capitalizing on these capabilities, from the use of personal mobile phones within strategic environments to hardened devices for tactical deployment. As DoD devices communicating on DoD networks, iPhones, Androids, Blackberries, and any other mobile devices will be held accountable to DoD inventory and security compliance policies. To date, SCAP has been foundational in helping to automate secure configuration management of Windows desktops and servers. This brief explores the capabilities of Mobile Device Managers (MDM) in enabling automated asset inventory and configuration compliance management of mobile devices and examines what role SCAP can play.

Mr. Tomasko is an Associate at Booz Allen Hamilton where he supports the Department of Defense (DoD) as an Information Systems Security Engineer (ISSE). Mr. Tomasko is the technical lead for the Compliance Management for Mobile Devices project to analyze policy and configuration guidance for mobile devices and looking for ways to automate the secure configuration management of these devices. He also serves in lead roles providing ISSE services to a variety of DoD programs. He has over 17 years of experience in communications, networking and information security. Mr. Tomasko holds an MSIT from Capella University and numerous professional certifications including CISSP-ISSEP, NSA-IAM, NSA-IEM, CCSP, CCNP, and PMP.

IT Security Threats Track

Potomac 5&6

The landscape of IT security threats continues to evolve at a rapid pace. This evolution is driven by the increasing sophistication of malicious attacks and the corresponding complexity of the security data generated from these attacks. Many of the emerging threats span multiple pre-existing classifications such as "malware" or "phishing", utilizing multiple disparate techniques to accomplish their goal. The success of an organizational security team is predicated upon the speed in which it can identify, collect, aggregate, share, and take action on incident information within a heterogeneous environment.

In related security domains, this increased complexity has driven the push towards automation of security objectives by creating standardized, machine-readable security languages as well as "continuous monitoring" and "continuous management" security architectures to manage the flow of this standardized data. Although the current security automation work continues to improve, how to capture standardized incident information in the context of complex IT security threats remains a significant challenge. This track will focus on describing the current and future landscape of IT security threats and highlight ongoing work to evolve and automate the incident handling processes designed to respond to these ongoing threats.

The Future Landscape of IT Security Threats – David O'Berry (McAfee)

This session will review the current events in the threat landscape and describe emerging trends that will need to be addressed in the near term.

Mr. O'Berry is a "reformed CxO/CIO currently working for 'The Dark Side' as a Strategic Systems Engineer for McAfee." He spent 19 years on the enterprise side as a network manager, Director of Information Technology Systems and Services and, most recently, Director of Strategic Development and Information Technology in the public sector. During that timeframe he was an advocate for standards-based networks and security working with groups like Trusted Computing Group and The Open Group to further those causes. Active within the industry, he currently holds CISSP-ISSAP, ISSMP, CISSLP, CRMP, among other certifications including old school certs like Master Certified Novell Engineer (a fact he tries not to mention very often). He calls himself a professional mutt because his background and experiences have been anything but a planned path throughout his career. Most recently he was honored as a ComputerWorld Top 100 IT Leader for 2011, a fact he attributes to the amazing team that surrounded him during his service in the public sector.

IT Security Insights: On the Frontline of the Threat Landscape - Marc Maiffret (eEye Digital Security)

The cost and consequences of maintaining security and compliance are steeper than ever. Exploits aren't slowing down and attackers have gotten smarter about how to penetrate networks. Plus, with new technical standards and government regulations, the urgency to secure and manage every aspect of the IT infrastructure increases even further.

In this presentation, eEye CTO and cofounder, Marc Maiffret, will give an overview of today's threat landscape and offer insights and guidance on the most recent high-profile attacks, such as "Night Dragon" and "Stuxnet." His candid talks are best known for cutting through hype and pinpointing what really matters to those in the trenches of IT security. Learn how to protect your critical IT assets and the data they hold, avoid common security pitfalls, and respond to today's ever-increasing threats and compliance requirements to minimize risk.

Mr. Maiffret co-founded eEye Digital Security where he currently serves as Chief Technology Officer. Marc is an industry expert in network security and has accepted three separate invitations to testify before the United States Congress on matters of national cybersecurity and critical infrastructure protection. Marc famously discovered the first Microsoft computer worm, "CodeRed" and was named one of People Magazine's 30 People Under 30. He has been featured for cover stories in Details, the Los Angeles Times, Entrepreneur, Inc., and USA Today in addition to numerous television appearances.

Anti-Phishing Working Group Adventures in Information Sharing: Now and for the Future – Pat Cain (APWG)

The Anti-Phishing Working Group (APWG) collects, shares, and metrics phishing and fraud information with its international correspondents. The mechanisms to collect, share, store, delete, correct and make statistics have evolved over the years for efficiency and volume concerns. As the system grows to include other types of eCrime, we are in a cat-and-mouse game of agreeing on a new data and format for sharing before the new eCrime appears needing to be shared. This presentation will explore the APWG's data clearinghouse model and its evolution from the historical system – what drove the changes, the solved challenges, open issues, and humorous experiences. Highlights will include current dilemmas on automated collection and sharing systems, proper data marking, and how to interact with other collection and sharing systems.

Mr. Cain is a Resident Research Fellow of the Anti-Phishing Working Group (APWG), and the President of The Cooper-Cain Group, Inc., a Boston, Massachusetts, USA-based computer and Internet security consultancy. He has been associated with information security development and operations for over twenty-five years and drives the APWG's data collection and sharing initiatives. He was previously the Security Advocate in the Office of the Chief Technology Officer, at Genuity Inc., a large Internet Service Provider.

He is a Certified Information Systems Auditor (CISA), a Certified Information System Manager (CISM), a member of the International Association of Privacy Professions, and an associate member of the American Bar Association. Mr. Cain participated in the FSTC Counter-Phishing project, led an effort in the IETF to standardize phishing and electronic crime reports (RFC 5901), participated in a US White House working group identifying and addressing the vulnerabilities of the Internet, and serves on a United Nations identity-related crimes experts panel.

The Evolution of Collective Intelligence – Wes Young (REN-ISAC)

SES is a project founded by the REN-ISAC community. Inception was funded by a U.S. Department of Justice grant in 2008 and with the cooperation and support of (Internet2, Internet2 CSI2 WG, Barely3am Solutions, Indiana University, Argonne National Laboratory (relation to Federated Model) and REN-ISAC members. The REN-ISAC currently serves 725+ members representing 300+ North American Universities as well as a handful of Universities abroad.

The objective of SES is to improve timely local protection against cyber security threats. This is done by means of real-time sharing of security event, infrastructure and malware related information within and between trusted federations using widely available internationally recognized standards (IDMEF, IODEF, IODEF+PhraudReport, ICSG malware, etc).

While the original implementation of SES (v1) focused mainly on machine generated intelligence (IDS, firewalls, honeypots, etc) and how to best leverage existing standards, our understanding of the threat intelligence problem has evolved. Our current road-map ("SES v2") takes a look at the "Collective Intelligence" concept and provides many real-world, operational examples of open-international standards. The Collective Intelligence Framework ("CI-Framework") is geared to normalize higher-level security intelligence (malware, infrastructure, url's, etc) into the various international standards in this space. Whether it comes from something like the Spamhaus DROP list, a private malware analyst partner, or even a local IDS, this framework focuses on unifying local repositories and client API requirements threat analysts need for making operational use of the intelligence (mitigation feeds, investigation research, incident response, etc).

With the evolution of the intelligence space over the last decade, we've also learned where the soft spots are in these standards and the ways in which we've proceeded to evolve them. The main goal of SES has been to not only facilitate the information sharing needs of the REN-ISAC community, but also to provide open-source implementation examples; glue-code for things like RT+IR, RT-IODEF as well as open source libraries for languages such as perl and python for the international security intelligence community. By lowering the barrier to entry for these existing standards, we help identify how they need to evolve to keep pace with current threats.

Mr. Young is the Principal Security Engineer at the Research and Education Networking Information Sharing and Analysis Center (REN-ISAC). Mr. Young is and has been the lead architect and developer behind the REN-ISAC SES project since its inception.

IETF MILE, Improving Incident and Information Sharing Standards - Kathleen Moriarty (EMC)

The Managed Incident Lightweight Exchange (MILE) working group in the Internet Engineering Task Force (IETF) is developing standards and extensions for the purpose of improving incident information sharing and handling capabilities. This talk will review the work in progress and how you can participate.

The work builds upon existing IETF standards including the Incident Object Description Exchange Format (IODEF) [RFC5070], which defines a standard format to exchange incident information and Real-time Inter-network Defense (RID) [RFC6045], which defines a messaging capability to securely exchange IODEF information while meeting policy and privacy requirements. Through growing use of these standards, gaps have been identified that the working group seeks to address to further improve incident information sharing and coordination. MILE has several initial objectives:

- provide additional guidance needed for the successful exchange of incident information for new use cases according to policy, security, and privacy requirements;
- produce several IODEF extensions to ensure specific use case needs are met such as data classification labeling, referencing structured security information from within incident reports, and the format for forensic data that may be shared in an investigation (computer and accounting); and
- create a generalization of RID for secure exchange of other relevant XML formats.

Ms. Moriarty is with the EMC Office of the CTO working on technology strategy and standards for Governance, Risk, and Compliance with a focus on incident response and related areas. Kathleen has been the primary author of multiple published standards and actively contributes to security standards activity in both the ITU-T and the IETF. Previously, as the practice manager for security consulting at EMC, Kathleen was responsible for oversight of key projects, and development of security programs, in addition to serving as the acting CISO of a global investment banking firm. Kathleen has also been the head of IT Security at MIT Lincoln Laboratory and the Director of Information Security at FactSet Research Systems. Kathleen holds a Masters of Science degree in Computer Science from Rensselaer Polytechnic Institute and a Bachelor of Science in Mathematics and Computer Science from Siena College.

Enabling Coordinated Incident Handling and Information Sharing – Tom Millar (US-CERT), Marcos Osorno (JHU-APL), Paul Cichonski (NIST)

Modern CSIRTs must process ever greater volumes of reports, indicators and remedies across broader and more complex networks of partners and customers. This panel session will present work to revise and extend existing incident handling guidance to answer the need for greater coordination and automated information exchange between CSIRTs in the GFIRST community and beyond, with the goal of generating discussion and soliciting community feedback.

Mr. Millar joined US-CERT in 2007 as a network analyst. Since then he has served as a senior watch officer, deputy operations manager, and chief of communications, playing a significant role in coordination and response to activities during major cyber events such as the 2007 Estonian DDoS attacks, Conficker's countdown, the US DDoS attacks of 2009 and several others. He holds a M.S. in Engineering Management and Systems Engineering from George Washington University.

Mr. Osorno is a mission continuity and operational neuroscience researcher at the Johns Hopkins University Applied Physics Lab. His research areas are mission-focused cyberdefense information sharing within complex, large-scale computer networks and understanding the neurological basis of situational awareness. Prior to his work at APL, Mr. Osorno worked for various government agencies as a continuity manager, at the United States Naval Academy as a knowledge collaboration researcher, and for the United States Army as an aeromedical evacuation officer.

Mr. Cichonski is an Information Technology Specialist at the National Institute of Standards and Technology (NIST). Mr. Cichonski supports the development of specifications relating to the Security Automation Program, aimed at standardizing the communication of IT security information. Mr. Cichonski is also researching ways to leverage W3C semantic technologies within IT security standardization efforts. Mr. Cichonski has a Bachelor's Degree in Information Sciences and Technology from Pennsylvania State University.

Vendor Product Highlights Track
Tidewater 2

This track provides presentations on various products that implement information security automation capabilities. Presentations will provide challenges, methodologies, approaches and solutions to various aspects of automating information security and demonstrate how various products support these methodologies and approaches and achieve solutions.

Cutting Through the SIEM/Log Management Vendor Marketing – A. N. Ananth (Prism Microsystems)

This session will explore how different solutions vendors have approached the problem from very different contexts and how to make the right technology decisions for your organization. Marketing departments are in overdrive; all claim their features and benefits will solve every problem you have. Learn how to define your requirements before you make your shortlist. We will explore two case studies involving both a civilian government customer and a DoD customer.

Mr. Ananth, the co-founder and CEO of Prism Microsystems, was one of the original architects of the EventTracker product offering, Prism's enterprise log management solution. With an extensive background in product development and operations for telecom network management, he has consulted for many companies on their compliance strategy, audit policy and automated reporting processes. He is a leading expert in IT compliance with over 20 years experience in IT-control and operations and speaks frequently on these topics. He was involved in product development for various companies including Ciena, Westinghouse Wireless and Equatorial Communications. He holds a MSEE from the University of Texas and remains active in strategic product direction at Prism.

Identifying & Sharing Threat Information with OpenIOC - Douglas Wilson (Mandiant)

Traditional methods of identifying evil on hosts and networks no longer work. Simple signatures and file characteristics are too easily circumvented by advanced intruders. Organizations need to be able to communicate how to find evil on their networks and hosts using a machine digestible format that removes human delay from intelligence sharing. In response to this problem, Mandiant has created the Open Indicators Of Compromise data sharing standard. Based off of Mandiant's years of industry leading incident response process, OpenIOC is what drives Mandiant's MIR product and industry leading IR. In an effort to assist the incident response community and ever-growing number of entities affected by intrusions, Mandiant has released the base OpenIOC schema and field tested extensions as Open Source, so that they can be used to track down artifacts of intrusion throughout a variety of enterprises.

This presentation will introduce the OpenIOC concept, show how OpenIOC can be used in different phases of the incident response process, and how Indicators can be written to not only find specific artifacts, but also to hunt down entire systems or classes of attacks, and ultimately find attackers by their overall methodology. These indicators can then be shared with other parts of an organization or external entities to communicate the threat artifacts that have been accumulated so that they can use them to find evil as well.

Mr. Wilson is a Principal Consultant at Mandiant. In addition to being a technology advocate for OpenIOC, he currently supports a contract doing research at the Information Assurance Directorate's (IAD) Center for Assured Software (CAS). Doug has over a decade of experience working in IT Security, as well as a background in Web Hosting and multi-tiered application architecture. Doug is also active in the Open Web & Application Security Project (OWASP) in Washington DC, including being the OWASP DC Chapter co-chair and an organizer of the AppSec DC Application Security Conference. Doug has spoken previously at the NSA High Confidence Software & Systems conference (HCSS), the Malware Technical Exchange Meeting (MTEM), and Shmoocon.

PowerShell Support in SCAP1.2 – Michael Tan (Microsoft)

This session will focus on a new definition, cmdlet_test, added in OVAL 5.10 windows definitions to support PowerShell for configuration management including problem space, business needs, PowerShell overview, design principles to integrate into SCAP. The session will demonstrate sample definitions and conclude with some thoughts on future development and how PowerShell is supported in Microsoft Security Compliance Manager, a key platform to deliver baselines for Microsoft products.

Mr. Tan is a senior program manager 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 to keep in compliance. Michael has been working on many security products since he joined Microsoft 14 years ago. Michael started working in Security and Compliance team 5 years ago; he has been focusing on security solutions for IT management, with part of the effort involving supporting SCAP.

Security Configuration Simplified with the Microsoft Security Compliance Manager (SCM) – Vlad Pigin (Microsoft)

If you are responsible for understanding, implementing or verifying security configurations for compliance, join us! Learn how the Security Compliance Manager (SCM) can help reduce your investment in security configuration research, accelerate the implementation of these settings in your Active Directory driven organization, and simplify the management of your "Gold Security

Baselines" across the organization. Our security experts will walk you through the features which will help you access and automate all of your organization's security baselines in one centralized location, show you how to leverage the Microsoft recommended security and compliance configurations for Microsoft Operating Systems and Applications, and how to verify drift using SCCM.

Mr. Pigin is a Program Manager in the Solution Accelerator for Security and Compliance (SA-SC) team. Some of the areas SA-SC works on include: Identity and Access Management, Security Management, Network Security, Operating System Hardening, Data Protection, and Shared Access. Vlad is currently working on Security Compliance Manager, a free tool from the Microsoft Solution Accelerator team that enables you to quickly configure and manage your desktops, traditional datacenter, and private cloud using Group Policy and System Center Configuration Manager. Before joining Microsoft, Vlad has driven early stage development and assembled talented teams of people for a number of businesses as a founder, manager, or board member. Vlad holds a Bachelor of Science degree in Information Systems Analysis and Bachelor of Arts degree in Business Administration from Lewis-Clark State College.

Using Vanguard Configuration Manager for Continuous Monitoring of NIST Security Controls on the IBM z/OS Operating System Environment - Brian Marshall (Vanguard Integrity Professionals)

This presentation will cover how the Vanguard Configuration Manager can be used to automatically scan your IBM z/OS environment for compliancy to the NIST Security Controls. During this presentation a high level overview of the NIST controls will be provided along with a demonstration of the capabilities of the Vanguard Configuration Manager to automate the checking of these security controls along with its built-in intelligence that will aid with any required remediation.

Mr. Marshall joined Vanguard in 2006, serving initially as Director of Research & Development until 2010. Marshall was the primary architect and visionary behind Vanguard Configuration Manager, and is an expert on NIST security standards. Prior to joining Vanguard, Marshall served 11 years in software development management at Computer Associates and Innovative DP Designs, Inc. He holds one shared patent on a method of reorganizing IMS databases online. Brian has been a professor of computer science at Solano College in California. He holds a B.S. Degree in Computer Science and an M.B.A., both from Sonoma State University. Brian is a frequent speaker at RUGS on various z/OS security and compliance topics, and is the Vanguard representative for OASIS, where he is helping to define communication protocols that will be applicable for cloud computing in the future.

Using OVAL for Information Security Application Integration – Marlon Gaspar (Modulo)

One of the most common requests in any information security product implementation is "how can you integrate with product X?" In this session, Modulo will describe how OVAL is being used to integrate applications in information security implementations. We will share step-by-step guides such as how OVAL can be used to integrate and harmonize risk scores between multiple products. Finally we will present a real-world case study demonstrating how OVAL can be used to integrate ABAP code scanning for an SAP application environment and integrate it into an IT GRC application using Modulo Risk Manager for a comprehensive approach to risk and compliance with continuous controls monitoring.

Mr. Gaspar is a senior Software Architect at Modulo. He is responsible for interoperability and integration of the product platform including the modSIC product and online community. He was the lead for Modulo's SCAP adoption and works with several standards groups towards reducing friction in identity and security systems integration. Marlon has over 10 years in IT Security and Risk Management software development.

Future of Global Vulnerability Reporting Track

Potomac 5&6

The rate of vulnerability discoveries and disclosures continues to accelerate at an ever-increasing pace. At the same time, the needs of the communities who consume and use vulnerability reporting information are evolving. The numerous current providers of cybersecurity vulnerability reports and related information each have their strengths and shortcomings, often related directly to the needs of specific communities. When viewed through the lens of a projected cybersecurity world one, two, or five years out, it appears that there is a need for something more, or at least different from, what is provided by today's vulnerability reporting mechanisms and capabilities.

This track will explore the current vulnerability reporting landscape using some well-known examples, and will attempt to project what that landscape might look like in the near- to mid-future. Following the panel discussions, a workshop will give interested attendees an opportunity to discuss these issues in more detail with fellow users and practitioners.

Panel: The State of Global Vulnerability Reporting – Tom Millar (US-CERT), Richard Struse (DHS), Steve Boyle (MITRE), Harold Booth (NIST), Art Manion (CERT/CC), Joe Hemmerlein (Microsoft)

The panel will explore the current state of vulnerability reporting and identification and highlight new and emerging use-cases and issues. Some of the issues that will be discussed include the need for global coverage of vulnerabilities, the value of unique identifiers, and the time and effort required to produce and publish reports.

Mr. Millar joined US-CERT in 2007 as a network analyst. Since then he has served as a senior watch officer, deputy operations manager, and chief of communications, playing a significant role in coordination and response to activities during major cyber events such as the 2007 Estonian DDoS attacks, Conficker's countdown, the US DDoS attacks of 2009 and several others. He holds a M.S. in Engineering Management and Systems Engineering from George Washington University.

Mr. Struse is the Deputy Director for Software Assurance in the Department of Homeland Security's National Cyber Security Division where he oversees efforts relating to the automation of Software Assurance. Prior to joining DHS, Mr. Struse was Vice President of Research and Development at VOXEM, Inc., where he was responsible for the architecture, design and development of a high-performance, extremely high-reliability communications software platform that is in use in telecommunications systems around the world. He began his technical career at Bell Laboratories where his work focused on tools to automate software development and the UNIX operating system.

Mr. Boyle is a Principal InfoSec Engineer in the MITRE Corporation's Cyber Security Technical Center, and the project leader for CVE. Steve has been messing around with computers since discovering a TTY-33 with an acoustic coupler in a high school classroom a very long time ago. During his career, he has worked and managed in nearly every facet of Information Technology and Information Security, both for MITRE internal operations and for MITRE sponsors. This has included software engineering, sysadmin, managing advanced technology development groups, running MITRE's Information Security project, and the creation of CVE. He has worked with and advised US Government sponsors in both DoD and the Intelligence Community. Steve keeps a box of blank IBM cards in his desk just in case punched card readers have a renaissance. He holds a B.S. in Computer Science from Boston University.

Mr. 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 a contributor to the development of the Security Automation Program specifications.

Mr. Manion is a senior member of the Vulnerability Analysis team in the CERT Program at the Software Engineering Institute (SEI). He has studied vulnerabilities and coordinated responsible disclosure efforts since joining CERT in 2001. Manion currently focuses on vulnerability discovery and other areas of applied research, including ways to improve vulnerability management, mitigation, and response. Prior to joining the SEI, Manion was the Director of Network Infrastructure at Juniata College.

Mr. Hemmerlein is a Security Program Manager at the Microsoft Security Response Center (MSRC). The MSRC is responsible for the investigation and remediation of security vulnerabilities across all Microsoft products and services worldwide, delivering security updates, guidance, education, and working with organizations, individuals and the industry to keep the information ecosystem secure. In this position, Joe has been managing security investigations and triage, and now concentrates primarily on security release and automation. Prior to joining the MSRC, he was involved with founding the Microsoft CSS Security Incident Response Team in EMEA, working both in Germany and the Netherlands, where he analyzed security incidents to determine cause and to apply countermeasures, provided forensics training and support to law enforcement, and worked across team boundaries to ensure that related internal tools and processes keep up with the pulse of the times. Joe is a CISSP since 2006, and has more than 10 years of international experience in the field of security investigations as well as platform and network infrastructure.

Panel: The Future of Global Vulnerability Reporting – Tom Millar (US-CERT), Richard Struse (DHS), Art Manion (CERT/CC), Kent Landfield (McAfee), Tim Keanini (nCircle), Steve Boyle (MITRE)

Informed by the issues raised in the first panel, this panel will discuss proposals to address new use cases and where appropriate,

the limitations of existing vulnerability reporting and identification schemes. The goal is to encourage solutions that address emerging global requirements for vulnerability identification and reporting in a sustainable and scalable manner.

Mr. Millar joined US-CERT in 2007 as a network analyst. Since then he has served as a senior watch officer, deputy operations manager, and chief of communications, playing a significant role in coordination and response to activities during major cyber events such as the 2007 Estonian DDoS attacks, Conficker's countdown, the US DDoS attacks of 2009 and several others. He holds a M.S. in Engineering Management and Systems Engineering from George Washington University.

Mr. Struse is the Deputy Director for Software Assurance in the Department of Homeland Security's National Cyber Security Division where he oversees efforts relating to the automation of Software Assurance. Prior to joining DHS, Mr. Struse was Vice President of Research and Development at VOXEM, Inc., where he was responsible for the architecture, design and development of a high-performance, extremely high-reliability communications software platform that is in use in telecommunications systems around the world. He began his technical career at Bell Laboratories where his work focused on tools to automate software development and the UNIX operating system.

Mr. Manion is a senior member of the Vulnerability Analysis team in the CERT Program at the Software Engineering Institute (SEI). He has studied vulnerabilities and coordinated responsible disclosure efforts since joining CERT in 2001. Manion currently focuses on vulnerability discovery and other areas of applied research, including ways to improve vulnerability management, mitigation, and response. Prior to joining the SEI, Manion was the Director of Network Infrastructure at Juniata College.

Mr. Landfield has spent 25+ years in software development, global network operations and network security arenas. He is currently 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 the catalyst in McAfee adopting SCAP component standards across three different security technologies. 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 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 IETF 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 other emerging standards working groups.

Mr. Keanini brings 20 years of technical expertise from both the information security and gaming industries, which provides him with unique insight into the dynamic problems customers face for risk management. As CTO, Tim's technical vision for nCircle has been shaped by his intimate understanding of both the "gaming mindset" which always takes into account an active opponent and his experience and respect for the ever-changing and complex nature of each customer's IT operations.

Mr. Boyle is a Principal InfoSec Engineer in the MITRE Corporation's Cyber Security Technical Center, and the project leader for CVE. Steve has been messing around with computers since discovering a TTY-33 with an acoustic coupler in a high school classroom a very long time ago. During his career, he has worked and managed in nearly every facet of Information Technology and Information Security, both for MITRE internal operations and for MITRE sponsors. This has included software engineering, sysadmin, managing advanced technology development groups, running MITRE's Information Security project, and the creation of CVE. He has worked with and advised US Government sponsors in both DoD and the Intelligence Community. Steve keeps a box of blank IBM cards in his desk just in case punched card readers have a renaissance. He holds a B.S. in Computer Science from Boston University.

Workshop: Issues in Global Vulnerability Reporting and Identification – Tom Millar (US-CERT), Richard Struse (DHS)

This two-session facilitated workshop will give interested participants an opportunity for a more in-depth exploration of the issues in global vulnerability reporting and identification as raised during the earlier panel discussions. The goal of this workshop is to facilitate and accelerate the discussion of practical solutions in global vulnerability reporting and identification and to explore promising avenues for their implementation.

Mr. Millar joined US-CERT in 2007 as a network analyst. Since then he has served as a senior watch officer, deputy operations manager, and chief of communications, playing a significant role in coordination and response to activities during major cyber events such as the 2007 Estonian DDoS attacks, Conficker's countdown, the US DDoS attacks of 2009 and several others. He holds a M.S. in Engineering Management and Systems Engineering from George Washington University.

Mr. Struse is the Deputy Director for Software Assurance in the Department of Homeland Security's National Cyber Security Division where he oversees efforts relating to the automation of Software Assurance. Prior to joining DHS, Mr. Struse was Vice President of Research and Development at VOXEM, Inc., where he was responsible for the architecture, design and development of a high-performance, extremely high-reliability communications software platform that is in use in telecommunications systems around the world. He began his technical career at Bell Laboratories where his work focused on tools to automate software development and the UNIX operating system.

Auxiliary Sessions Track
Potomac 5&6

These sessions were scheduled here due to limitations of available time in other tracks or addressing topics not supported in other tracks.

Efficiency in Security Audits - The Standards Journey of McAfee Policy Auditor - Lal Narayanasamy (McAfee)

This talk will trace the pioneering path adopted by McAfee Policy Auditor in aggressively adopting SCAP since its inception that has brought and continues to bring significant benefits to customers through automation and standardization of security audits. The successful adoption of continually evolving SCAP standards and the competitive edge it has brought to the product will be discussed. Case studies on how a standards-based audit tool like McAfee Policy Auditor has made security auditing easier for customer and brought about a "compliance is a way of life" mindset in organizations will be shared. McAfee's active participation in the SCAP community and how it continues to innovate through standards and contributes to the development of standards will be outlined through examples from McAfee Policy Auditor. In this content, some of the groundbreaking work that McAfee has done in security content and audit results localization, and "actionable findings" for detailed audit results will be discussed. Concepts around auditing for manual/procedural controls and performing surveys through emerging standards such as OCIL will be explored.

Mr. Narayanasamy is a Group Product Manager in McAfee's Risk and Compliance Business Unit (R&C BU) for McAfee Policy Auditor. He drives several key BU initiatives aimed at solidifying McAfee's position in Compliance and IT GRC in the public and private sector. He plays an active role in evaluating partnering and acquisition opportunities for the R&C BU, and integration of acquisitions. Lal joined McAfee in 2007 as a Senior Product Manager. Prior to joining McAfee, Lal was Senior Product Manager at VeriSign for the Enterprise SSL product line including the Managed PKI for SSL service where he played a lead role in the launch of Extended Validation (EV) SSL certificates for enterprises. Earlier stints include product management, marketing and corporate development roles in companies such as EDS, Honeywell International and the Mahindra Group. Lal has a master's degree in mechanical engineering from Oklahoma State University and an MBA from the University of Chicago Graduate School of Business.

Workshop: Implementing a Standards-Based Security Automation Program Outside of the Federal Government - Aharon Chernin (SCAP.com)

It's challenging to implement security automation outside of the Federal Government as there is no mandate to implement information security standards like SCAP. This workshop discusses how to build a business case for starting an automation program for vulnerability management, the requirements that should be in place, and the processes that must be implemented. We will also discuss performance and exposure indicators as well as how to integrate undetectable vulnerabilities into your vulnerability management program. We will see screenshots of an in-house, custom built automation tool that automates the vulnerability management process through the use of standards based content. We will close our discussion with thoughts on how we can improve the standards for usage outside of the federal government and the direction I would like to see us take in the future.

Mr. Chernin has over 15 years of IT experience. He has worn many hats during this time including: Unix Systems Manager, Web Application Developer, Vice President of Storage Deployment at JPMorgan, and now as a Security Automation Program Manager in the financial sector. He uses these diverse experiences to come up with unique solutions to real world security industry problems. Aharon is a standards and automation fanatic and an expert in vulnerability management. As such he built one of the first entirely automated and standards based vulnerability management programs in the private sector. Aharon also sits on the board for the OVAL standard. He is also one of the top contributors of vulnerability content to the MITRE OVAL repository with over 2,000 definition submissions. Aharon sees a future where all of information security is standards based, automated, and objective.