



SANS
2012 NATIONAL
Cybersecurity Innovation
CONFERENCE

Program Guide

The Baltimore Convention Center
Baltimore, MD | October 3-5, 2012

Co-located event with

8TH ANNUAL
IT Security Automation
CONFERENCE



Event-At-A-Glance

Wednesday, October 3, 2012

7:00-8:30am	REGISTRATION (<i>Pratt Street Lobby – 300 Level</i>)		BREAKFAST (<i>Ballroom III Foyer – 400 Level</i>)	
8:30-8:45am	WELCOME ADDRESS: Donna Dodson, NIST (<i>Ballroom III – 400 Level</i>)			
8:30-10:15am	GENERAL SESSION (<i>Ballroom III – 400 Level</i>) Keynote Address: Mobility and Security Automation: Are We Ready to Meet Emerging Cyber Challenges? <i>Speaker: Debora A. Plunkett, Information Assurance Director, National Security Agency</i> 2012 SANS National Cybersecurity Innovation Awards			
10:15-11:00am	BREAK (<i>Exhibit Hall – Level 100</i>)			
	NCIC <i>Ballroom IV</i>	Continuous Monitoring <i>Ballroom III</i>	Software Assurance <i>Room 340</i>	Solutions Track <i>Room 344</i>
11:00-11:45am	International Award Winner: Stopping Targeted Intrusions: The Australian Surprise - David Cottingham, Australian DSD	FedRAMP onto Cloud First: A CIO's Direction - Richard Spires, DHS	Software Assurance Automation for Supply Chain Risk Management - Joe Jarzombek, DHS; Ian Bryant, UK SSDRI; Bob Martin, MITRE	Intelligence-Driven Security: Advanced Threat & Continuous Monitoring -John McCumber
11:45-12:30pm	National Award Winners: Two Federal Agencies Implement Continuous Monitoring and Mitigation and Show Huge Risk Reduction - Matt Linton, NASA Ames Research Center; David Alexander & Michael Fluharty, CMS	Beyond A-130: Next Generation Federal Roles in Cyber - Karen Evans, US Cyber Challenge & Frank Reeder, NBISE	Empowering Automated Tools for Mitigating Egregious Software Weaknesses - Bob Martin and Steve Christey, MITRE	11:45-12:15 Hacking Databases: Exploiting The Top Database Vulnerabilities And Misconfigurations - Josh Shaul, Chief Technology Officer, Application Security Inc.
12:30-1:30pm	LUNCH (<i>Exhibit Hall – Level 100</i>)			
1:30-2:15pm	Federal Award Winners: Fighting Advanced Persistent Threats - Matt Myrick, Sr., Lawrence Livermore National Lab; John Dollen, NSA	More for Less: What Should be in the CISO Playbook - Tony Sager, SANS Institute	Results of the Static Analysis Tools Exposition (SATE) - Paul Black, Vadim Okun, and Tim Boland, NIST	1:30-2:30 Automating the 20 Critical Controls with a Full Life Cycle Security and Compliance Program - Andrew Wild, CSO, Qualys; Wolfgang Kandek, CTO, Qualys
2:15-3:00pm	Education Award Winners: Setting Standards in Cybersecurity Education - Steve Lafountain, NSA ADET	CMWG: The New Landscape of Opportunity - Tri-Chairs - Timothy McBride, Kevin Dulany, Nancy Lim; Dave Otto, DOJ	MAEC 2.0 Explored - Penny Chase, MITRE	2:30-3:00 SCAP, Mark Haase, Sr. Security Software Engineer, Lunarline, Inc.
3:00-3:45pm	BREAK (<i>Exhibit Hall – Level 100</i>)			
3:45-4:30pm	International Award Winners: Guidance for Implementing the 20 Critical Controls - CPNI & CESG	Cyber Effectiveness Measures & Thoroughly Modern Maturity (Model & Roadmap) - Dr. George Moore, Kim Watson, Richard Lippmann & Lisa Young	Malware Hunting with OVAL and MAEC - Ivan Kirillov, MITRE	3:45-4:45 CM, CAG, Cloud: The Perfect Storm? - Ned Miller, Symantec; John Bordwine, Symantec; Mark Ryland, Amazon; Matt Scholl, NIST; Dr. Eric Cole, SANS Institute
4:30-5:15pm	State Award Winners: Creating Ownership and Accountability Across the Security Team - Elayne Starkey, State of Delaware and DE DCISO Focus Team	Success Stories: Cloud Security at NASA - Matt Linton, NASA	Software Identification: Your IT Security Depends on It! - Steve Klos, TagVault.org	4:45-5:15 SecurCenter Continuous View -Ron Gula, Tenable
5:15-6:15pm	Networking Event in the Exhibit Hall – Level 100 (Food & Drinks provided)			

Event-At-A-Glance

Thursday, October 4, 2012

7:30-8:30am	REGISTRATION (Pratt Street Lobby – 300 Level)		BREAKFAST (Ballroom III Foyer – 400 Level)		
8:30-10:15am	GENERAL SESSION (Ballroom III – 400 Level) Keynote Address: Software Assurance: Updates from the Department of Homeland Security <i>Speaker: Mike Locatis, Assistant Secretary for Cybersecurity and Communications (CS&C), National Protection and Programs Directorate, US Dept. of Homeland Security</i> Government Priorities on Security Automation <i>Speakers: John Banghart, Program Analyst, Program Coordination Office, Office of the Under Secretary of Commerce for Standards and Technology, NIST; Phyllis Lee, NSA</i> The Bad Guys are Winning: Now What? <i>Speaker: Ed Skoudis, SANS Institute</i>				
10:15-11:00am	BREAK (Exhibit Hall – Level 100)				
	NCIC <i>Ballroom IV</i>	Continuous Monitoring <i>Ballroom III</i>	Incident Handling & Information Sharing <i>Room 340</i>	Trusted Computing & Security Automation <i>Room 342</i>	Solutions Track <i>Room 344</i>
11:00-11:45am	The Five Most Dangerous New Attacks - Ed Skoudis, SANS Institute	Civilian CONOPS - John Steufert, Director NCSD, DHS	Incident Response Orchestration in Advanced Threat Response: Opportunities and Challenges - Dennis Moreau, RSA	Trusted Computing Overview: Use Cases - Neil Kittleson, NSA	11:00-11:30am Security Intelligence Made Easy - Usman Choudhary, SIEM Security Manager, NetIQ
11:45-12:30pm	International Information Sharing: The Status and Implication of Data for Cloud Services - Moderator: Tony Summerlin, TA Summerlin; Tim Edgar, PM-ISE; Mike Howell, DOI; Mary Ellen Seale, DHS	DoD CONOPS - Kevin Dulany, DoD	An Introduction to TAXII: Trusted Automated eXchange of Indicator Information - Rich Struse & Tom Millar, DHS	Trusted Computing Overview: Standards - Mike Boyle, NSA	11:45-12:15 Advanced Situational Awareness (ASA) - Tom Kellerman, VP of Cybersecurity, Trend Micro
12:30-1:30pm	LUNCH (Exhibit Hall – Level 100)				
1:30-2:15pm	The Future of FISMA: A Look at the Legislative Landscape	Civilian FY 2013 Implementation - CMaaS - Dr. George Moore, DHS	The FS-ISAC and Financial Sector Cyber Intelligence Standards Adoption - Aharon Chernin, FN-ISAC	Security Automation Standards - Chris Salter, NSA	1:30-2:00 Beyond Continuous Monitoring, Multi-Layered Threat Detection and Response - Rob Roy, Federal CTO, HP Enterprise Security Products
2:15-3:00pm	Cloud Implementation, Continuous Monitoring & Policy Compliance Moderator: Dan Matthews, Information Innovators Inc.; Casey Coleman, GSA; Tim Schmidt, Dept. of Transportation	Civilian FY 2013 Implementation - Dashboard - Dr. Ron Rudman, State Dept.	Beyond Automation and Standards: The Next 10 Years of Information Sharing - Wes Young, REN-ISAC	Security Automation: Connecting your Silos - Lisa Lorenzin, Juniper Networks	2:15-3:15 The Impact of Hardware-Enhanced Security - David Marcus, Director, Advanced Research & Threat IntelligenceMcAfee
3:00-3:45pm	BREAK (Exhibit Hall – Level 100)				
3:45-4:30pm	White House Initiatives on Federal Information Security	Civilian FY 2013 Implementation - Priority Tools Phase I - Mark Crouter, MITRE	Information Sharing: What Works, Doesn't Work, and Still Needs to Work - Pat Cain, APWG	Network Access Control and Continuous Monitoring Standards - Jessica Fitzgerald-McKay, NSA	
4:30-5:15pm	Policy Wrap Up: What Else You Need for a Successful Implementation - Karen Evans, US Cyber Challenge; Julie Anderson, Civitas Group, Dan Matthews, Information Innovators Inc.	Success Stores: A Case for Change at VA - Andrew Rikarts, VA	Standardizing Cyber Threat Intelligence with the Structured Threat Information eXpression (STIX) - Sean Barnum, MITRE	SCAP and TNC - Eric Winterton, Booz Allen Hamilton	

Event-At-A-Glance

Friday, October 5, 2012

8:00-9:00am	REGISTRATION (<i>Pratt Street Lobby – 300 Level</i>)		BREAKFAST (<i>Ballroom III Foyer – 400 Level</i>)		
9:00-10:00am	ITSAC GENERAL SESSION (<i>Ballroom III – 400 Level</i>)				
	Keynote: The Basics and Beyond: Managing Security Effectively in the Rapidly Evolving IT Security Environments <i>Speaker: Tony Sager, SANS Institute</i>				
10:00-10:45am	BREAK (<i>Exhibit Hall – Level 100</i>)				
	NCIC <i>Ballroom IV</i>	Continuous Monitoring <i>Ballroom III</i>	Incident Handling & Information Sharing <i>Room 340</i>	Trusted Computing & Security Automation <i>Room 342</i>	Analytics & Mitigations: With Security Mitigation Enablers <i>Room 343</i>
10:45-11:30am	Implementing the Critical Security Controls : A Big Picture View - Dr. Eric Cole, SANS Institute; Rita Wells, INL	Success Stories: A Case for Change at DOJ - Kevin Cox & Dave Otto, DOJ	New Revisions to the NIST Computer Security Incident Handling Guidelines: Transforming Incident Coordination and Information Sharing Practices - Tom Millar, DHS, US-CERT	New BIOS Protections for Government Enterprise Clients - Bob Clemons, NSA	Information Assurance Metrics: Practical Steps to Measurement - James Tarala, SANS Institute
11:30-12:15pm	Learning from the Threats: Using Their Offense to Inform our Defense - Dr. Eric Cole, SANS Institute; Richard Bejtlich, MANDIANT; John Bordwine, Symantec; Sean Catlett, iSight	FedRAMP Incident Handling - Verdis Spearman, US-CERT	Incident and Indicator Exchange via Standards - Kathleen Moriarty, EMC	End-to-end Trust and Security Assertions for Mobile Platforms - Chris Daly, General Dynamics C4 Systems	How Automation Can Create Security Heroes and Eliminate the Conflicts Between Security and Operations Staff - Alan Paller, SANS Institute
12:15-1:15pm	LUNCH (<i>Exhibit Hall – Level 100</i>)				
1:15-2:00pm	Learning from the Users: Lessons Learned In Implementing the Critical Security Controls - Dr. Eric Cole, SANS Institute; Matt Linton, NASA; Virgle Gipson, NSA	CISO Roundtable - Steven Hernandez, HHS; Alma Cole, DHS; Jeffrey Eisensmith, ICE; Leo Scanlon, NARA; Gil Vega, DOE	Enhancing Risk Assessment with Threat Information - James Park, DoD	Integrated Mitigations Framework - Kevin Bingham, NSA	Analytic Methods for Network Security - Brian Keller, Booz Allen Hamilton
2:00-2:45pm	What Works: Effective Products and Services to Help Implement The Controls - Tony Sager, SANS Institute; Keren Cummins, nCircle	Success Stories: The Census Bureau - Jaime Lynn Noble and Tim Ruland, US Census Bureau	Digital Media Analysis at DHS - Roselle Safran, DHS	Developing SCAP Content the Open Source Way: the SCAP Security Guide Project - Jeff Blank, NSA	Practical Enumeration and Measurement of Cyber Threat Information - Dan J. Klinedinst, Carnegie Mellon University
2:45-3:30pm	BREAK (<i>Exhibit Hall – Level 100</i>)				
3:30-4:15pm	3:30-4:00pm Huge Risk Mitigation through Implementing the 20 Critical Controls at the U.S. Department of State: The Value of Dashboards and Daily Priority Lists - Dr. George Moore, DHS	CAESARS FE Update - Peter Sell, NSA	Global Vulnerability Reporting & Identification - Tom Millar, DHS; Harold Booth, NIST; Mark Bristow, ICS-CERT; Steve Christey, The MITRE Corporation; Kent Landfield, McAfee; Art Manion, CERT/CC; Rich Struse, DHS; Greg Witte, G2	SCAP Messages for Trusted Network Connect - Charles Schmidt, MITRE	Mitigating Insider Threats through Analytic-Enabled Security Automation - Grant Babb, Intel
4:15-5:00pm	4:00-4:45pm A Common Framework: Working Across National and Industry Standards - Tony Sager, SANS Institute	CAESARS Continuous Monitoring Prototype - Peter Sell, NSA		Practical Cyber Resiliency - Jeffrey Picciotto, MITRE	Finding the Signal in the Noise: Security Automation - David Marcus, McAfee
	4:45-5:00pm The Future of the Critical Security Controls - Tony Sager, SANS Institute				

Plenary Sessions

(Ballroom III)

Wednesday, October 3rd

- 8:30-8:45am **2012 Welcome Address**
Speaker: Donna Dodson, NIST, Division Chief of the Computer Security Division (CSD), Cyber Security Advisor, Acting Executive Director of the National Cybersecurity Center of Excellence (NCCoE), National Institute of Standards and Technology (NIST)
- 8:45-9:15am **Keynote Address: Mobility and Security Automation: Are We Ready to Meet Emerging Cyber Challenges?**
The National Security Agency's Information Assurance Director, Debora Plunkett, discusses current and emerging cyber security challenges. Ms. Plunkett will take an in-depth look at how mobility trends are affecting our nation's security posture and highlight the importance of security automation for information security across organizations and in mobile spaces. Ms. Plunkett will also discuss the essential importance of building and maintaining strong industry, government, and academic partnerships to combat the growing cyber threat, and stresses the strategic benefits of standards and information sharing.
Speaker: Debora Plunkett, Information Assurance Director, National Security Agency
- 9:15-10:15am **2012 SANS National Cybersecurity Innovation Awards**
*Presenters: Alan Paller, Research Director, SANS Institute
Debora Plunkett, Information Assurance Director, National Security Agency*

Thursday, October 4th

- 8:30-9:00am **Keynote Address: Software Assurance: Updates from the Department of Homeland Security**
Speaker: Mike Locatis, Assistant Secretary for Cybersecurity and Communications (CS&C), National Protection and Programs Directorate, US Dept. of Homeland Security
- 9:00-9:30am **Government Priorities on Security Automation**
*Panelists: John Banghart, NIS
Phyllis Lee, NSA*
- 9:30-10:15am **Keynote Address: The Bad Guys are Winning!: So Now What?**
With the continual release of zero-day exploits, ever-larger-scale botnets, and rampant spyware, attackers have compromised tens of millions of machines connected to the Internet. With clever attackers mixing social engineering, physical attacks, and phishing into their bag of tricks, their rate of successful penetration is both astounding and depressing. A central thesis of this talk is that a sufficiently determined (but not necessarily well-funded) attacker can compromise almost any organization with an Internet connection. The discussion will first analyze why this is so. We'll then look at the implications of such an environment for enterprises. How should information security priorities shift in light of this evolving threatscape and attack surface? What are the implications for system administrators, incident response teams, and even penetration testers and red team personnel? We'll also briefly look beyond the enterprise, and consider the military and national security issues associated with emerging threats and attacks, and the constantly evolving controversies around cyber war.
Speaker: Ed Skoudis, Fellow, SANS Institute

Friday, October 5th

- 9:00-10:00am **The Basics and Beyond: Managing Security Effectively in the Rapidly Evolving IT Security Environments**
Organizations have invested massive resources to defend their systems, but it seems like it is never enough, especially as the threat landscape continues to evolve. In this extraordinarily insightful talk, Tony Sager, the top cyber defense expert at the National Security Agency until he retired in June, will provide a roadmap to the future of cybersecurity. He'll focus on how automation fits, what data is needed and how it will be used, and he will introduce the other members of the new International Consortium of large companies and government agencies chartered to ensure that the 20 Critical Controls remain current with the evolving threat, that they remain authoritative, and that the best tools for automating them are identified.
Speaker: Tony Sager, Director, SANS Institute

NCIC

Ballroom IV (unless otherwise noted)

Wednesday, October 3rd

- 7:00-8:00am **Registration** (*Pratt Street Lobby – 300 Level*) & **Breakfast** (*Ballroom III Foyer*)
- 8:30-10:15am **ITSAC & NCIC Joint Plenary Sessions** (*Ballroom III – 400 Level*)
Keynote: *Speaker: Debora Plunkett, Director, Information Assurance Division, National Security Agency*
2012 National Cybersecurity Innovation Awards Presentation
- 10:15-11:00am **Networking Break in the Exhibit Hall – Level 100**
- 11:00-11:45 **International Award Winner: Stopping Targeted Intrusions: The Australian Surprise**
Only one national government has found and implemented techniques that actually block both intrusion vectors exploited in nearly all targeted intrusions nicknamed APT. Cybersecurity executives from the lead agency that proved it worked at scale are coming to the US exclusively to speak at NCIC and answer attendees' questions.
Speaker: David Cottingham, Australian Government, Department of Industry, Innovation, Science, Research, and Tertiary Education
- 11:45-12:30pm **National Award Winners: Two Federal Agencies Implement Continuous Monitoring and Mitigation and Show Huge Risk Reduction**
Two agencies have demonstrated that the extraordinary success of automated continuous monitoring and mitigation first proven at the U.S. Department of State can also be gained quickly and inexpensively in smaller organizations. NASA had instantaneous risk reduction and continues to gain the benefits of continuous monitoring and mitigation by simply altering vulnerability detection programs to bring responsibility directly to the sysadmins and technical staff – those who can actually fix the problems. The scoreboards are updated weekly and available to ALL sysadmins to view their own score in relation to those of their peers. Another 2012 honoree, The Centers for Medicare & Medicaid Services (CMS) comprise information systems in nearly 200 data centers, processing claims and payments with a value of over \$800 billion each year, for medical services rendered to over 100 million program beneficiaries and recipients. These agencies will show you the tools and techniques - some quite innovative - that they used.
Speakers: Matt Linton, IT Security Operations Lead, NASA Ames Research Center
David Alexander and Michael Fluharty, Centers for Medicare and Medicaid Services
- 12:30-1:30pm **Lunch in the Exhibit Hall – Level 100**
- 1:30-2:15pm **Federal Award Winners: Fighting Advanced Persistent Threats**
In this two-part briefing you'll learn about the Master Block List (MBL), a tool developed by the Department of Energy's Focused Advanced Persistent Threat (FAPT) group led by Lawrence Livermore National Laboratory. MBL allows multiple labs and plants to share block information in real time, increasing DOE's ability to leverage the intelligence of the collective as opposed to fragmented, individual pieces of information. Then hear about NSA's work with Non-Persistent Desktop Browsing (NPDB). This previously hypothetical approach now has been shown to actually work to stop nation states, cybercrime, and rogue actors, from socially engineering people browsing the Internet to attack and penetrate systems. This is a first line of defense to stop the exfiltration of valuable information for profit or espionage.
Speakers: Matt Myrick, Sr. Cyber Security Engineer, Lawrence Livermore National Laboratory
John Dollen, NPDB Technical Manager, National Security Agency
- 2:15-3:00pm **Education Award Winners: Setting Standards in Cybersecurity Education**
Although very few colleges have been graduating technically proficient and highly skilled students to fill the need for cyber operations missions, in the past year, the National Security Agency created a higher standard for colleges in cyber security operations and an innovative new incentive system that schools are competing to meet. For institutionalizing the program that enabled this program, and for rising to the very high new standard, the NSA ADET organization and the first four CAE-Cyber Operations schools – Dakota State University, Northeastern University, Naval Postgraduate School and University of Tulsa - are jointly awarded the 2012 National Cybersecurity Innovation Award. Other federal agencies with substantial cybersecurity responsibilities involved in hiring from the CAE schools have seen what is possible and are encouraging schools from which they recruit to raise their standards to a level nearly as high as the one deployed at the four model schools.
Speaker: Steve Lafountain, National Security Agency's Associate Directorate for Education and Training
- 3:00-3:45pm **Networking Break in the Exhibit Hall – Level 100**

NCIC (continued) **Ballroom IV (unless otherwise noted)**

Wednesday, October 3rd

- 3:45-4:30pm **International Award Winners: Guidance for Implementing the 20 Critical Controls**
Organizations who are implementing the 20 Critical Controls can look to guidance and education developed by the National Technical Authority for Information Assurance (CESG) and the Centre for the Protection of National Infrastructure (CPNI). CESG pulled from CPNI's work on the 20 Critical Controls to develop "10 Steps to Cyber Security," a launching pad for CISOs and their teams.
Speaker: Speaker from CPNI
- 4:30-5:15pm **State Award Winners: Creating Ownership and Accountability Across the Security Team**
Delaware's innovative Information Security Officer (ISO) certification program established a culture of security and advanced goals for risk reduction by formalizing the educational requirements and establishing minimum standards for all ISOs to meet. The program enables Delaware ISOs to demonstrate their knowledge of information security, enhances their career with increased credibility, and confirms their security commitment to their leadership team.
Speakers: Elayne Starkey, State of Delaware and Delaware DCISO Focus Team

- 5:15 - 6:15pm **Networking Event in the Exhibit Hall – 100 Level** (Food & Drinks provided)

Thursday, October 4th

- 7:30-8:30am **Registration** (Pratt Street Lobby – 300 Level) & **Breakfast** (Ballroom III Foyer)
- 8:30-10:15am **ITSAC & NCIC Joint Plenary Sessions** (Ballroom III – 400 Level)
Keynote Address: Software Assurance: Updates from the Department of Homeland Security
Speaker: Mike Locatis, Assistant Secretary for Cybersecurity and Communications (CS&C), National Protection and Programs Directorate, US Dept. of Homeland Security
Government Panel of Security Automation Priorities
The Bad Guys are Winning: Now What? - Ed Skoudis
- 10:15-11:00am **Networking Break in the Exhibit Hall – Level 100**
- 11:00-11:45am **Keynote: The Five Most Dangerous New Attacks**
Speaker: Ed Skoudis, Fellow, SANS Institute
- 11:45-12:30am **International Information Sharing: The Status and Implication of Data for Cloud Services**
Cloud-based information-sharing services make international collaboration efficient and thorough, but issues of privacy, governance, compliance and security of sensitive data can be thorny issues if not thought through and planned for in advance. Learn strategies, best practices, and pitfalls to avoid.
Moderator: Tony Summerlin, Founder, TA Summerlin
Panelists: Tim Edgar, PM-ISE
Mike Howell, DOI
Mary Ellen Seale, DHS
- 12:30-1:30pm **Lunch in the Exhibit Hall – Level 100**
- 1:30-2:15pm **Future of FISMA: A Look at the Legislative Landscape**
FISMA, now a decade old, needs a revamp to keep up with the accelerating adoption of continuous monitoring across government agencies. We'll examine the status of FISMA reform, including the bills that have been introduced and the likely Congressional intent of pending or passed legislation.
- 2:15-3:00pm **Cloud Implementation, Continuous Monitoring and Policy Compliance**
This session will discuss "real world" issues associated with the "cloud first" policy. The issues to be dissected include security, data retention as it affects FOIA, records management and privacy. We'll also focus on data gathering and how the change in reporting requirements is helping to move from paper writing reports to more actual risk management.
Moderator: Dan Matthews, EVP, Health IT, Information Innovators Inc.
Panelists: Casey Coleman, GSA
Tim Schmidt, Acting CIO, Dept. of Transportation

NCIC (continued)

Ballroom IV (unless otherwise noted)

Thursday, October 4th

3:00-3:45pm **Networking Break in the Exhibit Hall – Level 100**

3:45-4:30pm **White House Initiatives on Federal Information Security**

Everything is fair game in an election year. What would a change in leadership mean for federal information security? Alternately, what can we expect from the current administration as they enter a second term?

4:30-5:15pm **Policy Wrap Up: What Else You Need for a Successful Implementation**

What does it all mean, and where do we go from here? This session will put in perspective the day's policy discussions and prognostications, and offer practical advice for information security best practices, regardless of the political climate.

Moderator: Karen Evans, Nation Director, US Cyber Challenge

Panelists: Julie Anderson, Managing Director, Civitas Group

Dan Matthews, EVP, Health IT, Information Innovators Inc.

Friday, October 5th

8:00-9:00am **Registration (Pratt Street Lobby – 300 Level) & Breakfast (Ballroom III Foyer)**

9:00-10:00am **Keynote: The Basics and Beyond: Managing Security Effectively In the Rapidly Evolving IT Security Environment (Ballroom III)**

Organizations have invested massive resources to defend their systems, but it seems like it is never enough, especially as the threat landscape continues to evolve. In this extraordinarily insightful talk, Tony Sager, the top cyber defense expert at the National Security Agency until he retired in June, will provide a roadmap to the future of cybersecurity. He'll focus on how automation fits, what data is needed and how it will be used. And he will introduce the other members of the new International Consortium of large companies and government agencies chartered to ensure that the 20 Critical Controls remain current with the evolving threat, that they remain authoritative, and that the best tools for automating them are identified.

Speaker: Tony Sager, Director, SANS Institute

10:00-10:45am **Networking Break in the Exhibit Hall – Level 100**

10:45-11:30am **Implementing the Critical Security Controls - A Big Picture View**

Dr. Eric Cole will share the lessons learned by pioneering organizations that have made the Critical Controls an integral part of their defensive strategy and increased security without significant new resources. He will discuss the entire range of issues you must address: gaining Executive support for the Critical Controls within an organization; adapting the Controls to a specific Enterprise's needs; the selection of products and services; and on-going usage and maintenance of the Controls. He will be joined by Rita Wells of Idaho National Laboratory, who will present a worked example of how the Critical Controls can be adapted to a critical sector of the economy – the power sector.

Speakers: Dr. Eric Cole, Fellow, SANS Institute

Rita Wells, Idaho National Labs

11:30-12:15pm **Learning from the Threats: Using Their Offense to Inform our Defense**

In mature cybersecurity organizations, deep understanding of threats drives the risk assessment and aligns the defenses to effectively reduce risk in an enterprise. In this panel discussion, representatives of companies known for effectively monitoring the threat will share what they have learned about new attack techniques, how the threat is changing, and how this knowledge can be used to manage our defenses much more effectively.

Moderator: Dr. Eric Cole, Fellow, SANS Institute

Panelists: Richard Bejtlich, Chief Security Officer, MANDIANT

Sean Catlett, VP, iSight

12:15-1:15pm **Lunch in the Exhibit Hall – Level 100**

NCIC (continued)

Ballroom IV (unless otherwise noted)

Friday, October 5th

- 1:15-2:00pm **Learning from the Users: Lessons Learned In Implementing the Critical Security Controls**
The Critical Controls have moved beyond theory and have become an effective framework to improve security and reduce security incidents. From defending critical assets to meeting PCI compliance, organizations have shown that the controls work. In this panel discussion, organizations that are using the controls in an effective manner in both the government and commercial sectors, will discuss lesson learned and the keys to their success.
Moderator: Dr. Eric Cole, Fellow, SANS Institute
Panelists: John Bordwine, Symantec
Vergle Gipson, NSA
Matt Linton, Cyber Security Specialist, NASA Ames Research Center
- 2:00-2:45pm **What Works : Effective Products and Services to Help Implement The Controls**
Automation is essential to implement, manage, and scale the Critical Controls within an Enterprise. In this panel, leading solution providers will show how they help their customers implement the Critical Controls, make them part of the normal workflow of system and network management, and to use them as the basis for enterprise risk management processes.
Moderator: Tony Sager, SANS Institute
Panelists: Keren Cummins, nCircle
- 2:45-3:30pm **Networking Break in the Exhibit Hall – Level 100**
- 3:30-4:00pm **Huge Risk Mitigation Through Implementing the 20 Critical Controls at the U.S. Department of State: The Value of Dashboards and Daily Priority Lists**
No agency or company has been more thorough or successful in full-scale automation of the Critical Controls. To be more secure, organizations must have a way to find and fix the most critical problems every day. One of the key benefits of the Critical Controls is the ability to scale security and actually monitor status in real time and track longer term performance. In this talk, you will learn how dashboards and daily priority list reporting have been implemented and the impact on the ability to rapidly address threats and chinks in the armor. You'll hear how it was done, including the softer-side leadership techniques used to move from chaos to order in security for a globally deployed organization.
Speaker: Dr. George Moore, Technical Director of National Cyber Security Division, US Dept. of Homeland Security
- 4:00-4:45pm **A Common Framework: Working Across National and Industry Standards**
We are all overwhelmed by a multitude of security standards, requirements, frameworks, compliance regimes, oversight mechanisms, reporting schemes, etc. – at every level of detail, usually unsynchronized and often conflicting. But a new common theme is emerging – a focus on prioritizing defensive steps based on the most pressing threats; a need for much greater automation; and continuous measurement of security and threats driving a more dynamic defense. In this talk, panelists will discuss how they are working together to align their frameworks and how the Critical Controls can be used as a common baseline to create more focused, manageable, scalable, and secure Enterprises.
Moderator: Tony Sager, SANS Institute
- 4:45-5:00pm **The Future of the Critical Security Controls**
Where do we go from here? The controls are living guidance deserving of frequent updates and tuning. This talk will address the International Consortium and show how organizations can engage to make sure the controls remain authoritative, reflect the most current threat picture and meet the specific needs of participants.
Speaker: Tony Sager, Director, SANS Institute

Continuous Monitoring

Ballroom III (unless otherwise noted)

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.

Wednesday, October 3rd

11:00-11:45am **FedRAMP onto Cloud First: A CIO's Direction**

Federal Risk and Authorization Management Program (FedRAMP) is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. FedRAMP is governed by the FedRAMP Joint Authorization Board comprised of the CIOs from DHS, DoD, and GSA. FedRAMP addresses the need to reduce the time to market of Federal Cloud based systems and applications by performing the basic security assessment and authorization process of the cloud provider's offerings prior to contracted use by federal departments/agencies. The FedRAMP process provides a consistent security authorization process to all systems submitted, lowers the cost of entry to use a vendor's cloud offering, and provides for continually assessment and monitoring on behalf of the customers. FedRAMP is a means to an end goal of implementing a "Cloud First" strategy but does not alleviate the user from performing their own risk assessment and final decision to operate in a FedRAMP accredited system.

Speaker: Richard Spires, CIO, US Dept. of Homeland Security

11:45-12:30pm **Beyond A-130: Next Generation Federal Roles in Cyber**

As the threat to the cyber infrastructure on which the Federal government and the nation relies grows, the urgency of investing wisely in protection against, detecting, mitigating and recovering from cyber events takes on increasing urgency. Our adversaries are well-equipped and agile. Our defenses must be equal to the threat and they are not. Karen and Frank will discuss the dynamic nature of the cybersecurity threat and what that portends for Federal cybersecurity policy, practice and the alignment of responsibilities within the Executive Branch.

Speakers: Karen Evans, National Director, US Cyber Challenge

Frank Reeder, Director, National Board of Information Security Examiners

12:30-1:30pm **Lunch in the Exhibit Hall – Level 100**

1:30-2:15pm **More for Less: What Should be in the CISO Playbook**

The CISO is besieged by operational objectives, oversight imperatives, security directives, national initiatives, threat perspectives, technology electives, and of course, demanding executives - it's enough to elicit colorful expletives! In this talk, Tony will present his personal perspectives on how CISOs can maximize their effectiveness by: prioritizing and focusing on things that really matter (in terms of stopping the Bad Guys); using standards and automation to simplify management of the security basics and the sharing of threat information; and taking advantage of emerging community activities to build a defense that is dynamic and collaborative.

Speaker: Tony Sager, SANS Institute

2:15-3:00pm **CMWG: The New Landscape of Opportunity**

This panel discussion brings session participants face to face with a group of Government IT professionals covering the many facets of the Continuous Monitoring landscape. Participants will speak to and respond to participant input regarding strategic planning at the highest levels of the enterprise, policy and planning at every level of an organization, down to the practical issues involved with implementing a ConMon program at the operational level.

Speakers: Kevin Dulany, Chief, Risk Management Oversight Division, DCIO-CS/DIAP

Nancy Lim, Deputy Associate CIO, USDA

Timothy McBride, DHS

Dave Otto, IT Project Manager, US Dept. of Justice

3:00-3:45pm **Networking Break in the Exhibit Hall – Level 100**

Continuous Monitoring (continued)

Ballroom III (unless otherwise noted)

Wednesday, October 3rd

3:45-4:30pm

Cyber Effectiveness Measures & Thoroughly Modern Maturity

This session will discuss ways to measure progress toward security program maturity from essentially no security to full defensive security. The speakers will each briefly address the following topics, and then the panel will accept questions and comments.

- Kim Watson, NSA: The “Magic Quadrant” that defines basic program maturity levels.
- George Moore, DHS: The “Capability Areas” for a complete defensive security program within which maturity can be measured.
- Richard Lippman, MIT/LL: Developing objective metrics for measurement capability and risk.
- Lisa Young, SEI: Program vs. Process Maturity and initial results implementing the maturity metric concepts.

Speakers: Dr. Richard Lippmann, Senior Staff, MIT Lincoln Labs

Dr. George Moore, Technical Director of National Cyber Security Division, US Dept. of Homeland Security

Kim Watson, Technical Director, NSA/IAD

Lisa Young, Senior Engineer, CERT Carnegie Mellon University

4:30-5:15pm

NASA's IPOST vision: Low-Cost, High-Impact Security Information and Risk Scoring

The US State Department's experience with their IPOST tool showed the world that continuous monitoring was a viable and highly successful alternative to costly and slow C&A. However, many question whether agencies with tight budgets and heterogeneous environments can achieve similar results. This talk explores NASA's interpretation of IPOST as a tool for engaging and capturing the focus of security-critical technical staff to achieve rapid remediation of security issues with minimal cost.

Using free, open-source and inexpensive COTS software, NASA has developed an in house IPOST-like tool which utilizes core principles of gaming, social engagement and the natural sysadmin ego to provide staff with all the information they need to improve their security posture and encourage them to act upon it. It will also show how the tool can be utilized by security staff to identify systems or areas needing immediate attention or presenting great risk to the agency.

Speaker: Matt Linton, Cyber Security Specialist, NASA

5:15 - 6:16pm

Networking Event in the Exhibit Hall – Level 100 (Food & Drinks provided)

Thursday, October 4th

11:00-11:45am

Civilian CONOPS

Early consideration of continuous monitoring focused on protecting federal networks managed internal to cabinet Departments and Agencies. As threats to .gov related systems have increased, the urgency of adapting cyber diagnosis and mitigation strategies for protecting the full range of systems and applications under the purview of FISMA have come into focus – including the cloud. From these elements a concept of operations emerged that will guide the next several years of continuous monitoring development activities. In this briefing the origins of continuous monitoring will be applied to a strategy for dealing with known threats and vulnerabilities in phases. Matching expected tight budget times ahead, several suggestions for seeking out the highest return on investment projects drawing upon the multiple funding streams that underwrite federal cyber security improvements will be considered.

Speaker: John Streufert, Director National Cyber Security Division, US Dept. of Homeland Security

11:45-12:30pm

DoD CONOPS

This session will provide an overview of the usefulness of Continuous Monitoring within the Department of Defense from a Combatant Command's perspective, from a Service's perspective, from a National Security System's perspective, as well as from a Test and Evaluation perspective. This session will highlight data reuse supporting multiple focus areas (Certification and Accreditation and Cyber Defense).

Speaker: Kevin Dulany, Chief, Risk Management Oversight Division, DCIO-CS/DIAP

12:30-1:30pm

Lunch in the Exhibit Hall – Level 100

Continuous Monitoring (continued)

Ballroom III (unless otherwise noted)

Thursday, October 4th

- 1:30-2:15pm **Civilian FY 2013 Implementation - CMaaS**
As part of a new federal program to be funded in FY13, DHS plans to offer Federal Departments and Agencies (D/As) a Continuous Monitoring as a Service (CMaaS) along with sensor tools and a dashboard. In FY13 this program will focus on ensuring that the worst risks from unmanaged hardware and software, configuration settings (CCEs) and vulnerabilities (CVEs) are catalogue frequently, so that D/As can fix the worst problems first. The nature of this program for federal agencies has been presented in a series of meetings and webinars documented at the GSA FedBizOps site (search for: Diagnostics Industry Day).
This presentation will summarize this information for those who missed these longer presentations, and describe steps that DHS plans to help D/As make best use of these services. In addition it describes how others including the military, intelligence community, local/state/tribal government, and cloud service providers can use this procurement vehicle or adapt the technical specifications for their local use.
Speaker: Dr. George Moore, Technical Director of National Cyber Security Division, US Dept. of Homeland Security
- 2:15-3:00pm **Civilian FY 2013 Implementation – Dashboard**
This presentation will consist of a live demonstration of the latest version of iPost, the Department of State's Continuous Monitoring system, which has been in production and evolving steadily for 8 years. During an initial walkthrough of the different types of data being monitored and scored, the discussion will focus on the various issues that were faced. After that, the agenda will be fairly fluid according to the needs of the audience.
Speaker: Dr. Ron Rudman, Computer Scientist, The MITRE Corporation
- 3:00-3:45pm **Networking Break in the Exhibit Hall – Level 100**
- 3:45-4:30pm **Civilian FY 2013 Implementation - Priority Tools**
This session will explore the first phase in identifying and implementing critical, "highest priority" tools for use in developing and maintaining an accurate picture of an organizations' security risk posture. Attendees will gain a common understanding for using specific standards and identifying and leveraging the right tools and processes to automate and gather data across individual systems and departments for an enterprise wide, holistic perspective.
The discussion will focus on the continuous monitoring capabilities of Hardware and Software Asset Inventory Management, Security Configuration Settings, and Vulnerability Management as foundational underpinnings of enterprise security posture awareness and remediation.
Speaker: Mark Crouter, The MITRE Corporation
- 4:30-5:15pm **Success Stores: A Case for Change at VA**
Andrew will discuss the framework and technical solutions being implemented to solve the Information Security Continuous Monitoring challenge at the VA. Attendees will be presented with a detailed overview and encouraged to participate in an interactive discussion covering the successes and challenges of implementing Continuous Monitoring and Compliance Management solutions in one of today's most complex network environments and how the lessons learned by VA can be leveraged by everyone to drive fundamental, positive change within their organizations.
Speaker: Andrew Rikarts, SecureVA PM for Enterprise Visibility, US Dept. of Veterans Affairs

Friday, October 5th

- 10:45-11:30am **Success Stories: A Case for Change at DOJ**
This session will look at the development and implementation of the Department of Justice, Endpoint Lifecycle Management System (ELMS). ELMS is an Enterprise approach to situational awareness and continuous monitoring. The session covers practical lessons learned from planning, implementing, and operating an Enterprise suite of SAIR tools. The importance of strategic communication and an AGILE approach to project planning are discussed. The benefits and strengths of an Enterprise approach as well as the constraints and pitfalls to look out for are covered. The speakers will discuss the critical alignment between people, processes, and tools in bringing about a successful continuous monitoring program.
*Speakers: Kevin Cox, Assistant Director, US Dept. of Justice
Dave Otto, IT Project Manager, US Dept. of Justice*

Continuous Monitoring (continued)

Ballroom III (unless otherwise noted)

Friday, October 5th

11:30-12:15pm **FedRAMP Incident Handling**

Federal Government Information Technology (IT) is undergoing a massive transformation and just as the Internet changed the way the federal government does business and interacts with the public, cloud computing is changing the very landscape of the IT that enables it do so. While Cloud computing provides tremendous benefits to federal organizations and allows for more efficient productivity, collaboration and cost savings, many organizations could be reluctant to rely on the security of cloud computing services and solutions. The Federal Risk and Authorization Management Program (FedRAMP) provides a streamlined avenue for U.S. federal agencies to make use of secure cloud service offerings. The FedRAMP program provides an avenue for Cloud Service Providers (CSPs) to obtain a Provisional Authorization to do business with the Federal Government after undergoing a third-party interdependent security assessment that has been reviewed for accreditation by the FedRAMP Joint Authorization Board (JAB). By assessing security controls on the CSP candidate platforms, and providing Provisional Authorizations on platforms that have acceptable risk, FedRAMP enables federal agencies to forego the security assessment process for a multitude of known security controls. This presentation will explain how CSPs, under the FedRAMP, shall employ Incident Response controls and outline the critical stakeholder roles and responsibilities in the FedRAMP incident coordination process.

Speaker: Verdis Spearman, IT Specialist, US-CERT, US Dept. of Homeland Security

12:15-1:15pm **Lunch in the Exhibit Hall – Level 100**

1:15-2:00pm **CISO Roundtable on Continuous Monitoring**

Continuous monitoring presents an opportunity to greatly enhance mission effectiveness, lower cost and improve the efficacy risk-based cybersecurity programs throughout the Federal government. How should traditional cybersecurity programs and the role of the CISO be transformed with an infusion of reliable, objective information? This session gathers Federal CISOs from small and large agencies across government to discuss the challenges, opportunities and realities of continuous monitoring today and in the future. Expect lively discussion from a diverse panel of experts with unique missions, backgrounds and approaches to continuous monitoring.

*Moderator: Steven Hernandez, Chief Information Security Officer, Director, Information Assurance
Office of Inspector General, US Department of Health and Human Services*

*Speakers: Alma Cole, DHS
Jeffrey Eisensmith, ICE
Leo Scanlon, NARA
Gil Vega, DOE*

2:00-2:45pm **Success Stories: The Census Bureau**

This session will discuss the approach to implementation of policy, standards and technical solutions to address the shift to (ISCM) Information Security Continuous Monitoring at the Census Bureau. Attendees will be presented with an overview exploring the steps to establishing the program, challenges to implementing, and the technical decision making process of leveraging existing tools v. new technologies in the bureau's environment. The audience will hear first-hand, the lessons learned, best practices employed and the impact and results achieved on the road to change. The group will offer practical advice to organizations pursuing the additional protection that can be offered by implementing a continuous monitoring program over existing security strategies.

*Speakers: Jaime Lynn Noble, US Census Bureau
Tim Ruland, US Census Bureau*

2:45-3:30pm **Networking Break in the Exhibit Hall – Level 100**

3:30-4:15pm **CAESARS-FE Update**

This session will discuss the latest information regarding the enterprise Continuous Monitoring (ConMon) Technical Reference Model presented in NIST Interagency Report 7756 jointly developed by the NSA, DHS, and NIST. The goal of the model is to enable federated, interoperable ConMon implementations that support both operations and compliance. This session will provide information on important updates to the model, including the addition of an Enforcement Capability and Reporting Component. It will also present a more detailed view of the ConMon Reference Model Specification Layers, outlining how the subsystems collect, aggregate, and analyze the information received from higher and lower tiers within an organization, and how this provides situational awareness and supports risk-based decision making.

Speaker: Peter Sell, NSA

4:15-5:00pm **CAESARS-FE Continuous Monitoring Prototype: Lessons Learned**

This session will present the open source software development effort underway at NIST to build a prototype reference implementation of CAESARS-FE. The goal of the effort is to prove out the concepts defined in NIST IR 7756, IR 7799, and IR 7800, and to provide feedback on those specifications. In this presentation we will give an overview of the effort, discuss the approach and state of the prototype, and present the feedback that was generated as part of it. Finally, we will give a demonstration of the capability and discuss next steps.

Speaker: Peter Sell, NSA

Software Assurance

(Room 340)

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.

Wednesday, October 3rd

11:00-11:45am **Software Assurance Automation for Supply Chain Risk Management**

Achieving secure, dependable and resilient software requires that all parties share information so that the artifacts and implementations are specified, realized, and used in an appropriate manner, for which use of structured information sharing formats are vital. To better enable software stakeholders to reduce risks attributable to malware, vulnerabilities and exploitable software weaknesses relevant to specific business/mission domains and technologies, the Department of Homeland Security National Cyber Security Division (NCSA) Software Assurance Program has sponsored standardized security automation projects. The United Kingdom (UK) Software Security, Dependability and Resilience Initiative (SSDRI) public-private partnership (the approximate equivalent of the US DHS Software Assurance [SwA] initiative) has evolved an emergent view on the needs for information sharing "boundary objects" such as those arising from the DHS SwA-sponsored security automation efforts (addressed in MITRE's Making Security Measurable (MSM) activity) and the ways in which they interact. This panel discussion will address how standardized Software Assurance Automation is being used to better enable Software Supply Chain Risk Management.

*Speakers: Ian Bryant, Technical Director, UK SSDRI
Joe Jarzombek, DHS*

11:45-12:30pm **Empowering Automated Tools for Mitigating Egregious Software Weaknesses**

Eliminating the most important security weaknesses in your applications is a common goal whether you manage internal development activities, work with third party developers, or are developing a COTS application for enterprises. To-date, each vendor and team has been left to create their own method for prioritizing these types of issues. The Common Weakness Scoring System (CWSS) is working to create a standardized approach to this problem that would enable disparate measurements to be combined and compared so the overall weakness score for an application could be discussed and evaluated. This talk will cover the work to-date and the road ahead for this community effort within the CWE initiative. It will explain how CWSS is used to prioritize the most egregious exploitable software weaknesses relative to the respective domain and technology groups. CWSS provides a business value context that enables stakeholders to identify the top CWEs of most concern to them. Because each CWE has associated mitigation practices, the CWSS is used to prevent the respective CWE from being in the software because it enables a targeted focus. To better enable software stakeholders to reduce risks attributable to exploitable software weaknesses relevant to specific business/mission domains and technologies, the DHS Software Assurance (SwA)-sponsored Common Weakness Risk Analysis Framework (CWRAF) that uses the CWSS scoring criteria with CWE to provide consistent measures for prioritizing risk mitigation efforts and focusing secure coding practices, enables better informed decision-making and acquisition of more resilient software products and services. CWRAF enables targeted "Top-N" CWE lists that are relevant to the technologies used within specific business domains. Past 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 the exploitable weaknesses that are most significant to them given what their software does for their business.

*Speakers: Steve Christey, CVE/CWE Technical Lead, The MITRE Corporation
Bob Martin, Senior Principal Engineer, The MITRE Corporation*

12:15-1:15pm **Lunch in the Exhibit Hall – Level 100**

1:30-2:15pm **Results of the Static Analysis Tools Exposition (SATE)**

Software must be developed well to have high quality: quality cannot be "tested in." However auditors, certifiers, and others must assess the quality of software they receive. Static analyzers are capable and are developing quickly, yet, we need far more. In SATE IV tool makers ran their tools on selected target programs, and organizers analyzed the results. The target programs chosen include four large, open-source programs selected for having known (CVE-reported) vulnerabilities and also most of the Juliet test suite, almost 60,000 synthetic test cases in C/C++ and Java. This is an opportunity to hear the findings from SATE IV and to help shape the next exposition, SATE V.

Speaker: Aurelien Delaitre, Guest Researcher, NIST

Software Assurance (continued) (Room 340)

Wednesday, October 3rd

- 2:15-3:00pm **MAEC 2.0 Explored**
Malware Attribute Enumeration and Characterization (MAEC) is a language for attribute-based malware characterization, and can be used as a standardized way of describing malware in terms of its actions, behaviors, artifacts, and other relevant constructs. Version 2.0 of MAEC has recently been released, and incorporates a host of changes and refinements, the most notable of which is a redesigned object model achieved through the integration of the Cyber Observable eXpression (CybOX) schema. This track will provide an overview of this latest version of the MAEC schema and its capabilities, and will also go over some of the most relevant use cases to which it pertains. Also discussed will be the general methodology for creating instances of MAEC data, along with the freely available tools and utilities for assisting in this process.
Speaker: Penny Chase, Senior Principal Scientist, The MITRE Corporation
- 3:00-3:45pm **Networking Break in the Exhibit Hall – Level 100**
- 3:45-4:30pm **Malware Hunting with OVAL and MAEC**
Open Vulnerability and Assessment Language (OVAL) is a standard language for expressing how to assess and report upon the machine state of computer systems. MAEC describes malware in terms of its actions, behaviors, artifacts, and other relevant constructs. This tutorial will explore how MAEC and OVAL can be used to hunt for host-based indicators of the presence of malware. MAEC descriptions include host-based objects, attributes, and behaviors. OVAL Definitions with tests can be generated from MAEC descriptions, and these OVAL Definitions can be pushed to host-based security systems to check for malware artifacts on hosts. This capability is an example of how these incident indicator exchange standards can be integrated to enable automated incident response.
Speaker: Ivan Kirillov, Senior Infosec Engineer, MITRE
- 4:30-5:15pm **Software Identification – Your IT Security Depends on It!**
Software Identification and its impact on IT operations have never been more critical to organizations. This information is a fundamental foundation to security, logistics and compliance activities. Unfortunately, to date, authoritative and accurate software identification has been nearly impossible to achieve using existing tools that rely on the archeological approach of identifying software based on various artifacts of files or settings discovered on a computing device. The problem is magnified by the explosion of new devices (tablets, smart phones) and new computing paradigms (virtual machines, cloud computing, network centric devices such as Chrome books, etc).
This presentation provides the details you need to know on how to fix the issues of inaccurate software identification – not through using a tool, or service, but by working with your software vendor. Using today's technology and utilizing ISO standards, it is possible to get authoritative, identification of software including details on software package relationships that have never been a realistic possibility in the past.
Learn about this new approach to software identification as well as how this information can be used in the overall Security Content Automation Protocol (SCAP) environment to more completely automate your real-time monitoring systems.
Speaker: Steve Klos, Executive Director, TagVault.org
- 5:15 - 6:16pm **Networking Event in the Exhibit Hall – Level 100** (Food & Drinks provided)

Incident Handling & Information Sharing

(Room 340)

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 incident response is predicated upon the speed in which it can identify, collect, aggregate, share, and take action on incident information within a heterogeneous environment.

Incident Handling teams are evolving to operate in this ever-changing threat landscape by creating solutions that enable them to share incident data and response strategies with partner organizations who are experiencing similar types of attacks. This cross-organization coordination is allowing organizations to begin leveraging pooled cognitive-resources to solve certain aspects of incident response that may not be feasible for the organization to handle internally. This track is oriented towards those interested in understanding ongoing work in the incident handling information sharing space including: 1) the technical mechanisms and standards enabling the automation of information sharing, 2) the process models and evolving guidance for how to coordinate and share information across organizational boundaries, and 3) use cases and lessons learned from organizations who have had success using information sharing techniques to improve incident handling capabilities.

Thursday, October 4th

11:00-11:45am **Incident Response Orchestration in Advanced Threat Response: Opportunities and Challenges**

As Advanced Threat IR increasingly relies on more visibility and more expertise across the kill chain, the needs to coordinate evidence across sensing modalities, to manage forensics collection, to leverage indicators and to manage interaction across organizations/entities has created real opportunities to take advantage of orchestration technology. This session will describe several emerging opportunities to leverage orchestration in support of advanced threat incident response and approaches to addressing resulting challenges.

Speaker: Dennis Moreau, Senior Security Strategist, RSA

11:45-12:30pm **An Introduction to TAXII: Trusted Automated eXchange of Indicator Information**

TAXII is an initiative to involve public and private sector participants in the design, testing and development of a standardized, open, repeatable and sustainable way to automatically exchange indicator and incident information across sectors and organizations. TAXII's goal is ultimately to create the enabling technologies that will turn one organization's identification and analysis of suspicious activity into preventive measures across the broader community, as close to network speed as possible, forcing the adversary to expend significantly greater resources to avoid detection.

*Speakers: Tom Millar, Chief of Communications, US-CERT, US Dept. of Homeland Security
Rich Struse, Deputy Director for Software Assurance, US Dept. of Homeland Security*

12:15-1:15pm **Lunch in the Exhibit Hall – Level 100**

1:30-2:15 **The FS-ISAC and Financial Sector Cyber Intelligence Standards Adoption**

Sharing of cyber intelligence has primarily been done using human readable text and non-formatted binary documents. In order to automate, reduce costs, and increase accuracy, the Financial Sector has committed to standards adoption in this space. This discussion will focus on intelligence standards adoption in the private sector where there is no mandate to adopt standards. We will talk about building the case for adoption, the FS-ISACs role, operational aspects of sharing data using STIX, and give you some insight on just how we will attempt to get 4,200 member firms to join us in our adoption efforts.

Speaker: Aharon Chernin, Manager of Security Automation, Depository Trust and Clearing Corporation

2:15-3:00pm **Beyond Automation and Standards: The Next 10 Years of Information Sharing**

In the education sector, we've automated a lot of our data sharing using open standards and freely available technology over the years. This talk will discuss the road we've traveled, the problems we're solving now, where we expect the sharing landscape will look like in the coming decade and what technologies will be required to keep up with the demand at scale.

Speaker: Wes Young, Principal Security Architect, Research and Education Networking Information Sharing and Analysis Center (REN-ISAC)

3:00-3:45pm **Networking Break in the Exhibit Hall – Level 100**

Incident Handling & Information Sharing (continued)

(Room 340)

Thursday, October 4th

- 3:45-4:30pm **Information Sharing: What Works, Doesn't Work, and Still Needs to Work**
Many parties believe that a law or edict will just magically enable the sharing of suspicious or malicious activity data with others. Although an altruistic ideal – it never works that way. This talk will identify ideas that didn't work; things that seemed to work; and what didn't work in the APWG data sharing initiatives. A discussion of what still needs to be socially engineered to decree data sharing a success and some ideas on what to do with all the data collected will also be presented.
Speaker: Patrick Cain, Resident Research Fellow, APWG
- 4:30-5:15 **Standardizing Cyber Threat Intelligence with the Structured Threat Information eXpression (STIX)**
This session will give a brief introduction and overview of an ongoing DHS-supported, community effort to define a standardized, integrated information architecture for representing structured cyber threat information. It is intended to support cyber threat intelligence activities as well as cyber threat information sharing. The effort known as the Structured Threat Information eXpression (STIX) is a work in progress among a broad community of industry, government, academic and international experts. STIX is the underlying informational foundation for the Trusted Automated eXchange of Indicator Information (TAXII) effort and, as a whole or in parts, is actively being pursued as a basis for automation and information sharing within several active communities.
Speaker: Sean Barnum, Principal, MITRE

Friday, October 5th

- 10:45-11:30am **New Revisions to the NIST Computer Security Incident Handling Guidelines: Transforming Incident Coordination and Information Sharing Practices**
The latest revision of NIST's Special Publication on Computer Security Incident Handling (SP 800-61 rev.2) deleted a significant amount of material from older editions, including the familiar list of "incident categories" which had served as the foundation of many incident reporting and handling procedures over the last decade. This presentation will provide an overview of the substantial changes to the publication, describe the intent behind the changes, and discuss the resulting impacts and opportunities for cybersecurity practitioners throughout the government and private sector.
Speaker: Tom Millar, Chief of Communications, US-CERT, US Dept. of Homeland Security
- 11:30-12:15pm **Incident and Indicator Exchange via Standards**
The increased intensity and effectiveness of targeted attacks has created the need to share and exchange incident and indicator information for preparedness as well as for incident handling. The Managed Incident Lightweight Exchange (MILE) working group is continuing previous IETF work to expand the use cases covered by international standards to solve these problems. This standards work enables vendors a common method to securely exchange incident and indicator information between products, solving real use cases. This talk will provide a brief overview of the standards and the use cases driving these efforts. Lessons learned that are helping to shape the update and addition of standards through the consensus process of the IETF will be discussed as well as how attendees can get involved to ensure their use cases are solved through these standards.
Speaker: Kathleen Moriarty, GRC Strategy, Office of the CTO, EMC
- 12:15-1:15pm **Lunch in the Exhibit Hall – Level 100**
- 1:15-2:00pm **Enhancing Risk Assessment with Threat Information**
To date, information security continuous monitoring remains limited to assessment of vulnerabilities, and lacks the aspect of cyber threat information. This session will discuss the current state of continuous monitoring, where we need to head to include initiatives underway that characterize and communicate observed cyber threat, and ways to include that perspective in the assessment of risk.
Speaker: James Park, Program Manager - Network Assessments, NSA Information Assurance Directorate
- 2:00-2:45pm **Automated Malware and Forensic Analysis of Intrusion Incidents**
When an intrusion incident occurs, malware and forensic analysis can greatly assist a computer network defender in identifying indicators and producing actionable information. Automating this analysis can enable network defenders to conduct their examinations on malicious files and infected hard drives efficiently and effectively. This presentation will cover some of the tools, data, and procedures that can be utilized to incorporate automated analysis into incident handling and response.
Speaker: Roselle Safran, Digital Analytics Deputy Branch Chief, US-CERT
- 2:45-3:30pm **Networking Break in the Exhibit Hall – Level 100**

Incident Handling & Information Sharing *(continued)*

(Room 340)

Friday, October 5th

3:30-5:00pm

Global Vulnerability Reporting & Identification

The global cybersecurity community of practice continues to rely on vulnerability reporting, analysis and identification techniques which were standardized by US research and security organizations in the late 1990s and early 2000s. Today's incident handling, vulnerability identification, software assurance and continuous monitoring activities demand more from the vulnerability information "pipeline" than ever before, demanding coverage of industrial control systems, mobile devices, supply chain risks, cloud virtualization technologies and growing software markets overseas. This panel will clarify the challenges facing the community, identify the obstacles facing modernization of our vulnerability information sharing infrastructure, and elicit collaboration from the community in determining the way forward.

Moderator: Tom Millar, Chief of Communications, US-CERT, US Dept. of Homeland Security

Panelists: Harold Booth, NIST

Mark Bristow, Senior Analyst, ICS-CERT, US Dept. of Homeland

Steve Christey, The MITRE Corporation

Kent Landfield, McAfee

Art Manion, CERT/CC

Rich Struse, Deputy Director for Software Assurance, US Dept. of Homeland Security

Greg Witte, G2

Trusted Computing & Security Automation

(Room 342)

The cyber threat is constantly changing. Developing a trusted computing model that allows us to provide a robust and defensible domain is a fundamental step in reducing the effectiveness of cyber attacks. The first step in this model is having a hardware root of trust that allows us to ensure the integrity of our systems and the information that those systems provide to Security Automation and Network Access Control systems. These systems create a great deal of security data which are stored in a variety of databases, such as Metadata Access Point servers. Developing methods for analyzing this data to find intrusions or other anomalous behavior is the final step in the Trusted Computing process. This track will include presentations of use cases, standards, and implementations of trusted computing solutions. Attendees will gain insights into the current state of trusted computing technologies as well as how the US Government would like to see this technology evolve in the future to solve problems that we are seeing today.

Thursday, October 4th

11:00-11:45am **Trusted Computing Overview: Use Cases**

Network security affects everyone. In this session, we look at five diverse and unique organizations, ranging from the Department of Defense to manufacturing, that all successfully utilized elements of trusted computing to improve security and performance while lowering costs and risks.

Speaker: Neil Kittleson, Portfolio Manager, Dept. of Defense

11:45-12:30pm **Trusted Computing Overview: Standards**

The NSA Information Assurance Directorate (IAD) and the DoD have committed to using standards-based COTS products to secure their networks. But what are the top goals of the experts who write these standards? How can they collaborate with users and implementers? How important is interoperability? Drawing on interviews with 20 leading standards experts, you'll learn the best ways to optimize the standards process and make better use of standards to protect our networks.

Speaker: Mike Boyle, IAD Standards Technical Lead, NSA

12:30 - 1:30pm **Lunch in the Exhibit Hall – Level 100**

1:30-2:15pm **Security Automation Standards**

The benefits of security automation will not be achieved until the protocols, interfaces, and schema exist as a set of standards that can be required by government and other critical infrastructures in the products that they buy.

Speaker: Chris Salter, Mathematician, NSA

2:15-3:00pm **Security Automation: Connecting your Silos**

Managing security in today's ever-changing technology landscape is like being a farmer: it's all about managing your silos. Most IT organizations deploy many unique technologies from multiple vendors in an attempt to secure their infrastructure. Each of these technologies generally operates in its own silo, resulting in the duplication of basic functions across multiple appliances in multiple locations in the network. With security automation - enabling information to be shared in real time between heterogeneous collections of appliances - each new component added to the security infrastructure leverages value already in place in the environment.

Learn how to deploy a standards-based signaling bus to enable automated, intelligent network security decisions across a variety of technology components such as firewalls, anti-virus, intrusion detection / prevention, web application firewalls, vulnerability scanners, policy servers, CMDBs, SIEM, etc. Leverage metadata accessible through standard APIs that can be accessed for real-time actions and executed by multi-vendor products, including enterprise-specific data if needed. Maximize the value of your existing infrastructure by sharing information for dynamic, real-time visibility and control of your network.

Speaker: Lisa Lorenzin, Principal Solutions Architect - Security & Mobility, Juniper Networks

3:00-3:45pm **Networking Break in the Exhibit Hall – Level 100**

3:45-4:30pm **Network Access Control and Continuous Monitoring Standards**

NSA and the Trusted Computing Group are collaborating to develop new standards for endpoint health reports and continuous network monitoring. Learn about this exciting project and how it relates to current network access control standards from the TCG and IETF; what technologies already exist to enable this project; and future steps to ensure all endpoints are fully compliant with network policy.

Speaker: Jessica Fitzgerald-McKay, Network Security Analyst, NSA

Trusted Computing & Security Automation (continued)

(Room 342)

Thursday, October 4th

4:30-5:15pm **SCAP and TNC**

Trusted Network Connect (TNC) was developed by the international standards body to protect critical data flowing in your networks. TNC uses strong authentication and machine identity to assist in asset discovery and combined with SCAP can help with regulatory compliance. SCAP scanners implemented within the TNC environment can provide assurance of integrity and automate security checks to ensure continuous monitoring of the Enterprise assets.

Speaker: Eric Winterton, Senior Associate, Booz Allen Hamilton

Friday, October 5th

10:45-11:30am **New BIOS Protections for Government Enterprise Clients**

DHS and DOD require that new U.S. Government PC systems comply with new NIST standards for BIOS security: NIST Special Publication 800-147 (BIOS Protection Guidelines) and NIST SP 800-155 (BIOS Integrity Measurement Guidelines). This session explains why NIST created these guidelines, what they mean for PC client security, and what OEM vendors and network administrators must do to comply.

Speaker: Bob Clemons, Senior Computer Scientist, US Dept. of Defense

11:30-12:15pm **End-to-End Trust and Security Assertions for Mobile Platforms D52**

Enterprises considering the employment of a BYOD approach must carefully craft their BYOD policies to ensure that security posture is not negatively impacted. Due to the nature of BYOD, all aspects of the device management and usage are not under direct control of the enterprise, which creates enterprise concerns over the levels of trust and security compliance that can be achieved for BYOD. At the same time, device users need to be assured that the enterprise will not interfere or disrupt the personal or non-enterprise activities that are also supported by the mobile device. These concerns drive the need to have capabilities for the device that can manifest the trustworthiness and security compliance for the device. These manifestations need to be distinctive for each of the "personalities" that are present on the device. This presentation focuses on the end-to-end trust, security, and compliance assertions that need to be manifested for BYOD. The presentation describes an Assertion framework which identifies what trust and security assertions are needed for the BYOD scenario and how do TCG building blocks aid in formulating and securely transmitting these assertions.

Speaker: Chris Daly, Director, General Dynamics C4 Systems

12:15-1:15pm **Lunch in the Exhibit Hall – Level 100**

1:15-2:00pm **Integrated Mitigations Framework**

Based on the intrusion lifecycle, the Integrated Mitigations Framework attempts to identify critical goal areas for the Information Assurance and Computer Network Defense professional. These goals are intended to be understandable and engineer-able, helping to guide strategies and decisions for effective defense.

Speaker: Kevin Bingham, Global Mitigations Office, Chief, US Dept. of Defense

2:00-2:45pm **Developing SCAP Content the Open Source Way: the SCAP Security Guide Project**

The SCAP Security Guide Project is an open source project (<http://fedorahosted.org/scap-security-guide>) which provides SCAP content such as security guidance, baselines, and associated validation mechanisms for Red Hat Enterprise Linux 6. The project enables direct, transparent collaboration between government and industry. Using an open source approach to develop SCAP content was a natural choice for the Red Hat platform, and this also positions it for direct support by Red Hat. The project's significant XCCDF and OVAL content is designed for easy selection and reuse by major government agencies which issue baselines. Pooling interagency development efforts and collaborating directly with the platform vendor results in higher quality content and minimizes waste.

Speaker: Jeff Blank, Analyst, NSA

2:45-3:30pm **Networking Break in the Exhibit Hall – Level 100**

Trusted Computing & Security Automation (continued)

(Room 342)

Friday, October 5th

3:30-4:15pm

SCAP Messages for Trusted Network Connect

The Trusted Computing Group's Trusted Network Connect (TNC) working group has been developing a specification to describe the use of SCAP content for performing endpoint assessment in the TNC architecture. In this proposal, TNC specifies the network protocols and functional units of the architecture while SCAP languages are used to provide content formatting and assessment procedures. The goal of this work was to create a specification that closely follows the conventions of both SCAP and TNC vendors to provide a bridge between these two communities of practice. This document is being released for public comment to ensure it meets the needs and practices of users and vendors. This talk provides an overview of this proposed specification with the objective of preparing interested parties to review and comment on this work.

Speaker: Charles Schmidt, Lead Infosec Engineer, The MITRE Corporation

4:15-5:00pm

Practical Cyber Resiliency

This panel will focus on the near-term practical applications of cyber resiliency. Panel members will discuss the outcome of the recent 2nd Annual Secure and Resilient Cyber Architectures Workshop held 5/31-6/1/2012, emphasizing the concrete outcomes from that workshop along the three tracks: Terminology & Framework, Engineering Principles, and Metrics & Assessment. In addition, they will comment on recent successes and current challenges along multiple dimensions, including technical, policy, and acquisition/deployment.

Panelists: Laura Boehm DoD/CIO

Tom Llanso JHU/APL

Tom Longstaff NSA/R2

Bill Streilein MIT/Lincoln Labs

Analytics & Mitigations: With Security Mitigation Enablers

(Room 343)

Key enablers for Security Automation are Analytics and Mitigations! Only sound analytics built into robust Security Automation capabilities will effective and efficient response (Mitigations) to cyber events be possible. The increasingly large volumes of data collected as part of secure network management make the need for analytics a security automation mission imperative. Analytics allow network and systems owners to: (1) rapidly assess and quantify technical risks associated with new threats and vulnerabilities prior to deployment of mitigations; (2) develop operational risk scores based on this threat, vulnerability, and asset information rapidly; (3) effectively measure the effectiveness of mitigations employed in response to threats and vulnerabilities; and (4) inform root cause analysis and mitigation when countermeasure effectiveness decreases. The presentations in this track will explore analytic and mitigation techniques and tradecraft as enablers of Security Automation. Attendees will gain insights into operational and practical techniques and tradecraft they can use today to enhance security and reliability.

Friday, October 5th

10:45-11:30am **Information Assurance Metrics: Practical Steps to Measurement**

Show up to a security presentation, walk away with a specific action plan. In this presentation, James Tarala, a senior instructor with the SANS Institute, will be presenting on making specific plans for information assurance metrics in an organization. Clearly this is an industry buzzword at the moment when you listen to presentations on the 20 Critical Controls, NIST guidance, or industry banter). Security professionals have to know that their executives are discussing the idea. So exactly how do you integrate information assurance metrics into action in an organization and actually achieve value from the effort. Learn what efforts are currently underway in the industry to create consensus metrics guides and what initial steps an organization can take to start measuring the effectiveness of their security program. Small steps are better than no steps, and by the end of this presentation, students will have a start integrating metrics into their information assurance program.

Speaker: James Tarala, Senior Instructor, SANS Institute

11:30-12:15pm **How Automation Can Create Security Heroes and Eliminate the Conflicts Between Security and Operations Staff**

For more than a decade, security compliance specialists in far too many organizations have been perceived by CIOs and by IT operations staff as "security "Nazis." Now a breakthrough approach to continuous monitoring is changing their perceived status to "security heroes." The surprisingly cost effective approach uses existing tools in new ways. In this fast paced briefing you'll see how two different major federal agencies implemented the new approach, the lessons they learned along the way, the "secret sauce" that made it work, and you'll get an early look at the tools that are most effective in enabling the transformation

Speaker: Alan Paller, Director of Research, SANS Institute

12:15-1:15pm **Lunch in the Exhibit Hall – Level 100**

1:15-2:00pm **Analytic Methods for Network Security**

We will discuss several network security analytics that we have developed and deployed on real network data. The first analytic detects and correlates a particular indicator of compromise across air-gapped networks. The analytic consumes large sets of network logs and correlates various fields in the logs using Hadoop and Accumulo and provides local network defenders with near real time results. The second analytic examines network device data at the kernel level to detect the presence of malware that evades traditional antivirus. The analytic applies statistical and machine learning approaches to automate a labor intensive process, providing analysts with a prioritized list of network devices sorted by likelihood of infection. The third analytic detects anomalous activity in network user profiles and system behavior, indicative of insider threat or system compromise. The analytic applies statistical and graph-based techniques to identify and rank anomalies in raw network activity logs. The final analytic we will discuss identifies unauthorized users, anomalous data transfer, and spoofing of phone credentials on a secure mobile phone infrastructure. The analytics utilize machine learning and geo-spatial algorithms to detect anomalous use.

Speaker: Brian Keller, Ph.D., Lead Associate, Booz Allen Hamilton

Analytics & Mitigations: With Security Mitigation Enablers (continued)

(Room 343)

Friday, October 5th

2:00-2:45pm

Practical Enumeration and Measurement of Cyber Threat Information

Two of the biggest problems network and system owners have is enumerating and measuring cyber threat information. Moreover, solutions that do exist often do not scale and do not provide information that is easy to interpret. This talk will present experimental approaches being tested at CERT to apply formal research methods and intelligence analysis tradecraft to the problem of enumerating and measuring cyber threat information. Existing threat analysis usually relies on examining packets and malware while ignoring the sociological and behavioral components. For example, human networks, natural language processing, behavioral models and heuristics-based intrusion detection can all be used to predict and detect hostile actions. There is a wealth of publicly available information that can be mined, standardized and correlated for increased situational awareness and this presentation will show how this information can be leveraged into existing missions/operations.

Speaker: Dan J. Klinedinst, Senior Researcher, Carnegie Mellon University

2:45-3:30pm

Networking Break in the Exhibit Hall – Level 100

3:30-4:15pm

Mitigating Insider Threats through Analytic-Enabled Security Automation

Proactive Investigator is an end-to-end solution providing analytics for insider threat detection. Available under a GNU Public License, it provides components for automation of event collection, real-time queries on event streams, and loading and processing data. In addition to the automated process of applying risk scores to highlight the most concerning patterns, it provides a UI that integrates model exploration, drilldown analysis, and case management in a single UI. All this is necessary to turn billions of data points into actionable intelligence. This talk will share some of the experiences with using the tools, supporting insider threat detection at an enterprise level in a large organization.

Speaker: Grant Babb, SIEM Product Manager, McAfee, Inc.

4:15-5:00pm

Finding the Signal in the Noise: Security Automation

Measuring security posture in an automated and scalable way is non-trivial! The most effective option is often times down selecting, or reducing noise! Sound analytics with a focus on automation capabilities will effectively and efficiently reduce the response time to cyber events, e.g., malware, botnets, etc, be possible. This is exacerbated by the increasingly large volumes of data collected and analyzed. As such, network owners need analytics that facilitate rapid assessment and measurement of technical risks associated with threats to and on current and future assets. The presentations in this track will use examples to describe and discuss analytic techniques that find the signal in the noise and enable effective security posture measurement.

Speaker: David Marcus, Director, Advanced Research & Threat Intelligence, McAfee Labs Engineering

Solutions Track

(Room 344)

Wednesday, October 3rd

11:00-11:45am **Intelligence-Driven Security: Advanced Threat and Continuous Monitoring**

Does anyone believe that perimeter defenses are enough to protect businesses today? With massive amounts of digital information, Bring Your Own Device, Cloud, Big Data and more, our perimeter is more porous and harder to defend. It's imperative to rethink security in a more balanced way, devoting additional resources to detection and response. All while automating the proof of compliance process and focus on top to bottom Continuous Controls Monitoring through reporting across the enterprise, within individual organizations.

In this presentation, RSA, will discuss how an Intelligence-Driven Security model that evaluates risk, security spend allocation, and skills of the security team can enable businesses to get ahead of the latest threats through comprehensive visibility, actionable intelligence, and advanced security analytics for fast detection and investigation.

Speaker: John McCumber

11:45-12:15pm **Hacking Databases: Exploiting The Top Database Vulnerabilities And Misconfigurations**

According to the Identity Theft Resource Center, in the past year and a half, there have been close to 900 breaches and over 28,000,000 records compromised. With groups like Anonymous and LulzSec continuously hacking into major corporations and government agencies, do you wonder if you're next?

No organization, industry, or government agency is immune to the proliferation of complex attacks and malicious behavior. Ensuring database security is a priority for organizations interested in protecting sensitive data and passing audits.

Over the course of this presentation, a description of some of the sophisticated methods used in invading enterprise databases will be discussed, and the evolution of the security issues and features in each will be provided. A demonstration of popular attacks will also be presented.

The presentation will conclude by proposing essential steps IT managers can take to securely configure, maintain databases, and defend against malicious breaches entirely. Attendees will leave with a basic understanding of the most effective methods for protecting their data, an enterprise's most prized asset, from attackers today and in the future.

Attendees will:

- Learn how organizations, through an integrated defense strategy, can effectively manage their database risks across large, heterogeneous database environments with automated controls
- Understand the common vulnerabilities and misconfigurations used to attack databases
- Methodologies and best practices on how to implement actionable plans to protect enterprise database assets

Speaker: Josh Shaul, Chief Technology Officer, Application Security Inc.

12:15-1:15pm **Lunch in the Exhibit Hall – Level 100**

1:30-2:30pm **Automating the 20 Critical Controls with a Full Life Cycle Security and Compliance Program**

The CSIS 20 critical controls are known for driving effective security programs across government agencies, establishing guidelines for security professionals working to ensure the confidentiality, integrity and availability of an organization's information technology assets. The automation of these controls can drastically lower costs while helping organizations achieve greater success in their implementations. In this session, we will discuss best practices for automating these controls by leveraging a full life cycle IT security and compliance program.

Speakers: Andrew Wild, CSO, Qualys

Wolfgang Kandek, CTO, Qualys

2:30-3:00pm **SCAP Sync**

Lunarline's SCAP Sync is a search engine and content repository for SCAP content. SCAP Sync crawls SCAP content from multiple original sources (including NIST and MITRE) and then syndicates that content in several convenient formats for both security practitioners as well as application developers who are looking to use SCAP content in their own applications.

For security practitioners, SCAP Sync provides a central location to search and view SCAP content in a user-friendly format. You don't need to know technical details like XML or CVSS – we handle all of that stuff for you. Our goal is to demystify SCAP and to make it more relevant and useful for the average security practitioner.

In addition to making SCAP content more useful for security practitioners, SCAP Sync also makes SCAP content more useful for application developers. SCAP Sync has a full REST API that gives you the ability to retrieve any single piece of SCAP content in machine-readable format, and to be confident that the content is the most-up-to-date content available.

Speaker: Mark Haase, Sr. Security Software Engineer, Lunarline, Inc.

Solutions Track (continued) (Room 344)

Wednesday, October 3rd

3:00-3:45pm **Networking Break in the Exhibit Hall – 100 Level**

3:45-4:45pm **CM, CAG, Cloud: The Perfect Storm?**

The promise of Continuous Monitoring, Consensus Audit Guidelines and the Cloud suggest that the “collective we” have a strategy towards achieving a better security posture and overall situational awareness. This panel will discuss if these initiatives intersecting today represent the definition of success or “the perfect storm” with many unknowns ahead. Panel members will share their respective views of success stories, challenges and an over the horizon view of what to expect next.

Moderator: Ned Miller, Director of Public Sector Strategy, Symantec

Panelists: John Bordwine, Symantec

Mark Ryland, Amazon

Matt Scholl, NIST

Dr. Eric Cole, SANS

Thursday, October 4th

11:00-11:30am **Security Intelligence Made Easy**

For security professionals who must answer the question, “How secure are we?” but are overwhelmed with the constant change and complexity of the computing environment and emerging threat profiles, NetIQ® Sentinel 7 is a powerfully simple Security Information and Event Management (SIEM) solution built to help protect sensitive information assets and achieve regulatory compliance while cutting through the rapid cycle of change in enterprise IT. When “Continuous Monitoring” is a priority assuring that you can accurately assess risk is critical.

This presentation will highlight NetIQ Sentinel 7’s ability to increase your visibility and understanding of potential threats and speed remediation without the need of extensive training or expertise—all while gaining the security intelligence and control you need to secure your enterprise with greater confidence and assurance like never before.

Speaker: Usman Choudhary, Senior Director of Engineering, NetIQ

11:45-12:15pm **Advanced Situational Awareness (ASA)**

APTS have long relied upon information security tunnel vision in order to maintain persistence within agencies networks. We must spin the chess board and learn from the advanced tactics utilized in cyber campaigns. ASA will discuss best practices regarding incident response in 2013. Areas of focus will be how to incorporate threat intelligence; attack path mapping and multi-rule event correlation into a cohesive strategy to thwart digital insiders. In addition the presenter will compare and contrast eastern European and East Asian cyber killchains.

Speaker: Tom Kellermann, VP of Cyber Security, Trend Micro

12:15-1:15pm **Lunch in the Exhibit Hall – Level 100**

1:30-2:00pm **Beyond Continuous Monitoring, Multi-Layered Threat Detection and Response**

Continuous monitoring has enabled many organizations to take a more proactive approach to security. For years, Government organizations labored to fulfill better security with compliance checklists. While we all know that compliance does not equal security, recent observations of breach data indicate that over 90% of the organizations breached were subject to a specific compliance mandate, but were NOT in compliance. The purpose of this session is to look beyond continuous monitoring to a new era of integrated defenses that work collaboratively to exchange vulnerability and threat information at multiple layers in a business or mission system to better detect active attacks and automate effective responses to minimize consequences.

Speaker: Rob Roy, Federal CTO, HP Enterprise Security Products

2:15-3:15pm **The Impact of Hardware-Enhanced Security**

Almost all information security products are focused on detecting and mitigating attacks at the operating system plane and above. The McAfee® DeepSAFE platform, developed jointly by McAfee and Intel, is focused on preventing attacks below the OS. This session will focus on how hardware-assisted security will improve an enterprise’s security posture and play a major role in securing mobile devices in the future.

Topics include:

- In-Depth Nuts and bolts of preventing attacks and why it fails at the OS level
- Using the hardware-assisted security methodology and framework

Speaker: David Marcus, Director, Advanced Research & Threat Intelligence, McAfee

Speaker Biographies

Grant Babb, McAfee

Grant Babb (CISSP) has worked for a decade in information security, in both management and technical security domains. Working across many industries including manufacturing, software, and healthcare, he has worked a risk analyst, information security investigator, and IT auditor. His recent work has been in security automation, specifically advanced analytics for threat detection; he is a recognized expert on Insider Threat and its detection. His current role is a product manager at McAfee, Inc. for the SIEM product line. He holds a BA in Economics and Mathematics from the University of Texas at Austin and is currently pursuing a graduate program in Applied Mathematics at the University of Illinois Urbana-Champaign.

Sean Barnum, MITRE

Sean Barnum is a Cyber Security 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 US government sponsors throughout the national security, intelligence community and civil domains. He has over 25 years of experience in the software industry in the areas of architecture, development, software quality assurance, quality management, process architecture & improvement, knowledge management and security. He is a frequent contributor, speaker and trainer for regional, national and international cyber security and software quality publications, conferences & events. He is very active in the Cyber Security community and is involved in numerous knowledge standards-defining efforts including the Cyber Observable eXpression (CyBOX), the Structured Threat Information eXpression (STIX), the Common Attack Pattern Enumeration and Classification (CAPEC), the Malware Attribute Enumeration and Characterization (MAEC), the Common Weakness Enumeration (CWE), the Software Assurance Findings Expression Schema (SAFES), and other elements of the Cyber Security Programs of the Department of Homeland Security, Department of Defense and NIST. He is coauthor of the book "Software Security Engineering: A Guide for Project Managers", published by Addison-Wesley. He is involved in the cyber security related standards efforts of ISO, OMG and IETF, among other international standards bodies. He also acted as the lead technical subject matter expert for design and implementation of the Air Force Application Software Assurance Center of Excellence (ASACoE).

Richard Bejtlich, MANDIANT

Richard Bejtlich is Chief Security Officer at MANDIANT. He was previously Director of Incident Response for General Electric, where he built and led the 40-member GE Computer Incident Response Team (GE-CIRT). Prior to GE, he operated TaoSecurity LLC as an independent consultant, protected national Security interests for ManTech Corporation's Computer Forensics and Intrusion Analysis division, investigated intrusions as part of Foundstone's incident response team, and monitored client networks for Ball Corporation. Richard began his digital security career as a military intelligence officer in 1997 at the Air Force Computer Emergency Response Team (AFCERT), Air Force Information Warfare Center (AFIWC), and Air Intelligence Agency (AIA). Richard is a graduate of Harvard University and the United States Air Force Academy. He wrote "The Tao of Network Security Monitoring" and "Extrusion Detection," and co-authored "Real Digital Forensics." He also writes for his blog (taosecurity.blogspot.com) and Twitter (@taosecurity).

Kevin Bingham, DoD, Chief of the Global Mitigations Office, NSA/IAO

Kevin Bingham is the Global Mitigations Office Chief in NSA/IAO's Fusion, Analysis, and Mitigations Deputy Directorate. Kevin's organization is focused on effective and scalable cyber defense capabilities for the Dept of Defense and the Federal Government. Previously, Kevin spent four years as the CND Architect for the Department of Defense supporting Computer Network Defense strategy and architectural efforts. In addition, he spent six years with the NSA Red Team, serving in positions as on-net Operator, Wireless LAN vulnerabilities Team Lead, Assessment Team Lead and Operations Branch Chief. Military time included ten years in the Air Force as a C-130 Navigator in the Pacific and as an Instructor at the Air Force Undergraduate Navigator Training School at Randolph AFB Texas. He holds a Bachelor's of Science Degree in Mechanical Engineering from Texas Tech University and a Master of Science Degree in Computer Information Systems from St. Mary's University in San Antonio, TX."

Jeffrey Blank, NSA

Mr. Blank is a technical director for the Network Components and Applications Division of the Technology and Systems Analysis Office within NSA's Information Assurance Directorate. He holds a bachelor's degree from the University of Kentucky, and a master's degree from the University of Maryland, College Park, both in Computer Science. In addition to the longstanding goal of automated checking, he hopes that SCAP can drive timely completion of certification and accreditation activities and also relate these to security.

Harold Booth, NIST

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.

Mike Boyle, NSA

Mike Boyle has worked at NSA for 22 years, mostly in the Information Assurance Directorate. His background is math and cryptography, but he has branched out over the years into Trusted Computing and Platform Security. Recently Mike was named the IAD Standards Technical Lead and has used his powers wisely and justly.

Mark Bristow, DHS/ICS-CERT

Mark Bristow is an Incident Responder/Analyst at the Department of Homeland Security's Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). Mark has been with ICS-CERT since its creation in 2009 and previously supported DHS's Control Systems Security Program.

Ian Bryant, UK SSDRI

Ian Bryant is Professional Engineer, currently assigned as the Technical Director of the Software Security, Dependability and Resilience Initiative (SSDRI), the UK's public-private partnership for Making Software Better. He has been involved with Information Security for most of his career as a public servant, in a variety of organisations (including Defence, Policing and the Cabinet Office) and roles (including Accreditation, Architecture/Engineering, Incident Response and Policy). He was intimately involved with various SSDRI predecessor activities, including leading the original Cabinet Office (CSIA) study on Secure Software Development and the subsequent Special Interest Group (SIG) on Standards, and being Technical Manager for the Pilot Operation of the then CSIA Claims Tested Mark (CCT Mark) Scheme. In the wider Standards context, he is a member of several BSI Committees, for the panel on Information Security (IST/033) acting as Lead UK Expert on Architecture (also ISO/IEC Rapporteur); Cybersecurity; Incidents / Investigations / Evidence; and Software, and is also a member of the ETSI MTS SIG on Security. He Co-Chairs the National Information Assurance Forum (NIAF), was lead Information Security specialist for the recent European Commission (EC) funded MS3i / NEISAS Projects, and is a Visiting Lecturer at a number of Universities.

Patrick Cain, APWG

Patrick Cain is a Resident Research Fellow of the Anti-Phishing Working Group (APWG), and the President of The Cooper-Cain Group, a Boston, Massachusetts, USA based Internet security consultancy. He has been involved in information security development and operations for over twenty-five years and drives the APWG's data collection and sharing initiatives. 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 led an effort in the IETF to standardize phishing and electronic crime reports (RFC 5901), participates in many data-sharing initiatives, and serves on a United Nations identity-related crimes experts' panel.

Sean Catlett, iSIGHT Partners

Sean is the Vice President of iSIGHT Partners, Inc. running their commercial threat intelligence and cyber risk management business. Previous to that he was the CISO at Betfair in London, the world's biggest online betting community and one of the fastest and most resilient trading platforms available on the internet, where he rebuilt their security capability and helped the company manage a severe and now public cyber-attack. Sean joined Betfair from Barclays PLC where he was Global Head of Threat and Vulnerability Management for the Barclays Global Retail and Commercial bank. In that role he transformed the function by creating strategies and new capabilities in data loss prevention, information security and privacy incident response and security assessment. Prior to joining Barclays Sean was a Senior Vice President at Bank of America leading their global Security Monitoring and Response team. Sean built a creative and innovative security R&D team which delivered millions of dollars in customer value year over year through detection of electronic fraud and attacks. Prior to financial services, he worked as the VP of Technology at Streamwaves, Inc. where he created a streaming music delivery system responsible for the world's first legal delivery of on-demand subscription streamed music from all 5 major record labels. Sean graduated with honors from University of Texas at Dallas with a B.S. in Business Administration.

Penny Chase, The MITRE Corporation

Penny Chase is the Department Head for Human Language Technology within MITRE's Center for Integrated Intelligence System's Information Technology Center. She has led MITRE and government-sponsored projects in developing structured representations for malware and threat information, security visualization, software assurance, malware analysis, reverse engineering, software architecture and design pattern recovery, network penetration testing, legacy database encapsulation, machine learning, and discourse-based natural language interfaces. Penny chairs the DHS/DOD/NIST Software Assurance Forum Working Group on Malware and leads the Malware Attribute Enumeration and Characterization (MAEC) project. Penny received her Bachelor of Arts in Mathematics and History from the State University of New York at Binghamton and Masters degrees in History of Science and in Computer Science from Harvard University.

Aharon Chernin, DTCC

Aharon Chernin currently works as the Manager of Security Automation at the Depository Trust and Clearing Corporation. Aharon is also a member of the OVAL board and is the chair of the FS-ISAC Security Automation Working Group.

Usman Choudhary, NetIQ

A seasoned executive with over 17 years experience with expertise in systems architecture and development of innovative solutions for real-time and high volume problem domains. He currently serves as Senior Director of Engineering for Security Management products at NetIQ, a leading provider of software infrastructure solutions. He previously worked with innovative startups such as e-Security, which invented SIEM technology, and led the development of the SIEM space in its early days. Through subsequent acquisitions he has pioneered SIEM in memory correlation capabilities, intrusion detection and identity integration, and advanced statistical analytics. During his tenure, he has also developed and managed SSO and Cloud Security products. Today he leads development of NetIQ's Security Portfolio, which includes Sentinel (SIEM solution), Change Guardian (FIM solution) and Secure Configuration Manager (Compliance Solution).

Robert Clemons, US DoD

Bob Clemons has worked in Information Assurance at NSA for his entire 26-year career. For the past ten years his primary area of expertise has been virtualization. Then for some reason he got involved in BIOS.

Kevin Cox, U.S. Dept. of Justice

Kevin Cox, PMP, CISSP, is Assistant Director for Information Security Technologies for the CIO's IT Security Staff of the Department of Justice. In that role, he works with his team and with Department Bureaus and Components to implement enterprise security solutions that strengthen the Department's IT security posture and provide near real-time awareness. Prior to his current role, he served as the program manager for the Department's Computer Emergency Readiness Team (DOJCERT) and served as a project manager and Unix system administrator for a major server consolidation project. Kevin holds an MA in Public Policy from West Virginia University and an MA in Divinity from the University of Chicago.

Speaker Biographies (continued)

Mark Crouter, MITRE Corp.

Mark Crouter is a Senior Principal Cybersecurity Engineer and Department Head of the Information Assurance Practice in MITRE's Center for Connected Government. Mr. Crouter joined MITRE in 2004 and has supported the Department of Homeland Security and other federal agencies in network and information security management. He has over 20 years management experience in federal government information technology and telecommunications projects and IT security risk management. Prior to joining MITRE, Mr. Crouter managed technical projects at Impact Innovations Group, Booz Allen Hamilton, and the U.S. Navy. His previous clients include the Departments of Defense, Veterans Affairs, Justice, Energy, and Education; U.S. Navy; Federal Bureau of Investigation; and the General Services Administration. Mr. Crouter received a Bachelor of Arts degree from the University of Virginia, Master of Science in Systems Management from the University of Southern California, and a Graduate Certificate in Information Security Management from The George Washington University. He is a graduate of the Naval Postgraduate School and the U.S. Naval War College and is a Certified Information System Security Professional.

Chris Daly, General Dynamics C4 Systems

Currently a Senior Technology Strategist for General Dynamics C4 Systems, Mr. Daly has over thirty years of experience as an analyst, consultant, architect, principal, business development executive, and technical director. Mr. Daly is responsible for security strategies, architectures, solutions, and vendor ecosystem development for the GD C4S federal marketplace with emphasis on cybersecurity, trusted technologies, mobility, and cloud security. Mr. Daly has served in several strategic capacities dealing with clients and industry including current co-Chair of the Trusted Computing Group's Trusted Mobility Solutions Work Group, member of the NSA Enduring Security Framework BIOS Integrity Management Panel and Mobile Device Integrity Panel, and, various government and industry work groups on SOA security, cybersecurity, and IA metadata. Also, Mr. Daly is the GDC4S representative to the DoD Partnership for Cybersecurity Training.

Aurelien Delaitre, NIST, SATE IV Organizer, Software and Systems Division, National Institute of Standards and Technology

Aurelien Delaitre's experience with IT security ranges from consulting, to cell phone forensics, to software assurance. In 2009, he joined the NIST SAMATE team, where his work focuses on static analysis. He is an organizer of the Static Analysis Tool Exposition (SATE) and a contributor to the SAMATE Reference Dataset (SRD).

Donna Dodson, NIST

Donna Dodson is the Division Chief of the Computer Security Division (CSD), the Cyber Security Advisor, and the Acting Executive Director of the National Cybersecurity Center of Excellence (NCCoE) at the National Institute of Standards and Technology (NIST). Donna oversees the CSD cybersecurity research program to develop standards, guidelines, technology, tests and metrics for the protection of unclassified Federal information and information systems. Through partnerships with industry, Dodson also ensures NIST cybersecurity contributions help secure the Nation's sensitive information and systems. This includes establishing public-private collaborations for accelerating the widespread adoption of integrated cybersecurity tools and technologies. Prior to her roles in management, Dodson led projects in cryptography, key management and authentication. Dodson received a Department of Commerce Gold Medal and three NIST Bronze Medals. She was a recent Fed 100 Award winner and included in the top 10 influential people in government information security.

John Dollen, National Security Agency

Mr. Dollen is a Civilian DOD employee conducting Enterprise Information Assurance Architecture and Systems Engineering for the National Security Agency. He has 30 years experience in national security systems, having worked in nearly all roles involved in the system development life cycle. In the past year he provided leadership in the role of Technical Manager for a Joint Technical Demonstration for the Joint Chiefs of Staff, namely the Non-Persistent Desktop Browser. Mr. Dollen has a degree in Information Systems Management from the University of Maryland and he holds several certification related to his field.

Kevin Dulany, DCIO-CS/DIAP

Kevin Dulany is the Chief, Risk Management Oversight Division at the Defense-wide Information Assurance Program (DIAP) Office supporting the Deputy Chief Information Officer for Cybersecurity. His duties include the oversight of DoD Continuous Monitoring and Risk Scoring efforts, the DoD's Certification and Accreditation (C&A) transformation efforts, the DoD's Computer Network Defense Service Provider Program, and the DoD's support to the Federal Risk and Authorization Management Program (FedRAMP) and Cloud Security. Mr. Dulany also tri-chairs the Federal Continuous Monitoring Working Group, the CNSS Continuous Monitoring and Compliance Assessment Working Group, and provides support to other CIO Council's Information Security and Identity Management Committee (ISIMC) led efforts (e.g. US Government Anti-Spear Phishing Strategy). Mr. Dulany is a retired U.S. Marine (Master Sergeant) who held the IA Technician Military Occupational Specialty (MOS) and was the USMC Information Assurance Chief for his final 4 years prior to retirement.

Karen Evans, National Director, US Cyber Challenge

Karen Evans serves as the National Director for the US Cyber Challenge, a nationwide program focused specifically on the cyber workforce. She serves as a Voice of Authority for Safegov.org, an on-line forum specifically focused on cloud computing policy issues. She is also an independent consultant in the areas of leadership, management and the strategic use of information technology. She retired after nearly 28 years of federal government service with responsibilities ranging from a GS-2 to Presidential Appointee as the Administrator for E-Government and Information Technology at the Office of Management and Budget within the Executive Office of the President. She oversaw the federal IT budget of nearly \$71 billion which included implementation of IT throughout the federal government.

Jessica Fitzgerald-McKay, National Security Agency

Jessica Fitzgerald-McKay works in the Mitigations Group within NSA/IA/D. In that organization, she leads the work being done on Trusted Network Connect technologies and is the group's primary interface with the Trusted Computing Group. Of NSA's trusted computing experts, she is distinguished by having the longest last name.

Mark Haase, Lunarline, Inc.

Mark Haase is a Sr. Security Software Engineer with Lunarline, Inc. and the lead software engineer for SCAP Sync. He has over 4 years of experience building security automation software, including FISMA, NIST RMF, SCAP, and POA&M automation software. Mr. Haase is also involved with secure software lifecycle development and independent source code audits.

Joe Jarzombek

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

Brian Keller, Booz Allen Hamilton

Brian Keller is a Lead Associate at Booz Allen Hamilton where he has applied statistics and data mining techniques to solve analytics problems for various federal government and commercial clients for the last three years. His work often involves the use of big data technologies such as Hadoop and NoSQL databases.

Tom Kellerman, Trend Micro

Prior to Trend Micro, Kellermann served as Chief Technology Expert for Air Patrol, a leader in intelligent enterprise mobility solutions. He is a professor at American University's School of International Service and a Certified Information Security Manager (CISM). Additionally, Kellermann is a member of the Committee of the Financial Coalition Against Child Pornography. He also co-authored the book "E-safety and Soundness: Securing Finance in a New Age."

Ivan Kirillov, MITRE

Mr. Kirillov is the technical lead behind the MAEC effort and the primary author of the MAEC schemas and tools. Over the past few years, he has worked closely with the broader anti-malware community to gather requirements and develop models and standard techniques for better and more accurate malware characterization. He has been working in the cyber security realm at MITRE after earning an M.S. in Computer Science from Georgia Tech in 2009.

Neil Kittleson, DoD

Mr. Neil Kittleson is a technology strategist in the NSA/CSS Commercial Solutions Center (NCS). Prior to this position Mr. Kittleson served as the High Assurance Platform (HAP) Program Manager where he led the successful deployment of the first release of the program and the development of the second release. Prior to joining the National Security Agency in 2008, Mr. Kittleson held a number of senior consulting positions with firms in San Diego and the Washington DC area where he helped clients successfully design, deliver, and support large scale information technology and satellite communication projects. Prior to consulting, Mr. Kittleson served as a U.S. Navy Supply Corps Officer for six years with deployments in support of the Persian Gulf War and the NATO peacekeeping efforts in the Bosnian War. Mr. Kittleson graduated from Miami University, in Oxford, Ohio, with a Bachelor of Arts degree in Political Science."

Dan Klinedinst, Carnegie Mellon / CERT

Dan Klinedinst is a Member of the Technical Staff at Carnegie Mellon University's CERT program. Klinedinst is CERT's senior technical SME for the DHS Risk and Vulnerability Assessment program. This program provides vulnerability assessment, threat modeling and penetration testing services to federal civilian agencies. Klinedinst has extensive experience in penetration testing, tool development and systems engineering. He is a regular speaker at international security conferences, an organizer of the BSides Pittsburgh conference and author of multiple open source security tools. Klinedinst previously worked as a senior security engineer for Lawrence Berkeley National Laboratory.

Steve Klos, TagVault.org

Steve is the executive director of TagVault.org, a program of IEEE-ISTO. He is also the convener of ISO/IEC 19770-2:2009 and a member of the ISO/IEC JTC1/SC7 US Technical Advisory Group (TAG) and Work Group 21 (WG21 – targeting SAM Standards). Steve is the recipient of multiple industry awards and certifications in Software Asset Management including being an IAITAM Fellow and a Microsoft Certified Professional with a Software Asset Management Competency.

Kent Landfield, McAfee/Intel

Kent Landfield has spent nearly 30 years in software development, global network operations, advanced network security research and product development arenas. At McAfee, Kent built and managed the global Risk and Compliance Security Research teams. His responsibility included producing the content supplied with McAfee's remediation, policy auditing, vulnerability management and NAC products. Kent was the catalyst in getting SCAP component standards adopted as the basis for product and content integration across three different technologies within McAfee. He initiated the first large scale commercial SCAP Content development team and content production architecture in the world. His team achieved the first localization of SCAP content, delivering localized content in eleven languages enabling SCAP products to be sold into a true global market. Currently as Director of Content Strategy, Architecture and Standards for McAfee Labs Kent is an active leader and participant in the SCAP community and in the Continuous Monitoring efforts NIST is pursuing. Kent is one of McAfee's Principal Architects for advanced research. He has been involved with the development of security standards since the POSIX working groups in the late 1980s. He has also been involved with standards development in the Internet Engineering Task Force, the Trusted Computing Group and the Trusted System Interoperability Groups, in addition to others. He is one of the original CVE Editorial Board Members, an OVAL Board member and is active in emerging security automation standards working groups.

Speaker Biographies (continued)

Nancy Myoung-Sook Lim, USDA

Nancy Lim joined the Office of the Chief Information Officer at the Department of Agriculture in April of 2012. She serves as the Deputy Associate Chief Information Officer (DACIO) for USDA's Agriculture Security Operations Center (ASOC) as of August 2012. She is responsible for providing executive leadership in security operations, architecture, and risk management, and is responsible for securing USDA networks and systems by collecting, analyzing, integrating and sharing information among the USDA component services. Ms. Lim will coordinate cyber-security situational awareness, resources, and reporting for USDA organizations and personnel in order to protect USDA programs, information, and assets. Ms. Lim presently serves as one of the chairs to the Federal Continuous Monitoring Working Group (CMWG) under the Federal Chief Information Officer Information Security and Identity Management Committee (ISIMC). Ms. Lim received a Bachelor of Science from the College of William and Mary. She also holds current professional credentials on information security, Certified Information Systems Security Professional (CISSP).

Richard Lippmann, MIT Lincoln Laboratory, Cyber Systems and Technology Group, MIT Lincoln Laboratory

Dr. Lippmann is a Senior Staff at MIT Lincoln Laboratory. Recent work focuses on developing new approaches for risk assessment, adversary modeling, and security analysis of large enterprise networks and both dynamic and static code analysis to detect vulnerabilities. In the past he led the first formal evaluation of intrusion detection systems, applied machine learning and neural network approaches to many computer security problems, and performed research in automatic speech recognition, speech perception, speech training aids for the deaf, and signal processing for hearing aids. He has authored or co-authored more than 100 papers, reports, or books in the above research areas, has been a Distinguished Lecturer for the IEEE Signal Processing Society, received the first IEEE Signal Processing Magazine award for an article entitled "An Introduction to Computing with Neural Nets," and recently received one of the two yearly Technical Excellence Awards from MIT Lincoln Laboratory. Selected papers are available at: <http://www.ll.mit.edu/mission/communications/CST/biographies/lippmann-bio.html>.

Michael W. Locatis, Department of Homeland Security

Michael W. Locatis joined the Department of Homeland Security as Assistant Secretary of Cybersecurity and Communications in April 2012. As a part of this collaboration, in his role as the A/S of CS&C, Mr. Locatis oversees CS&C's large portfolio of programs to protect the dot-gov domain. Included among these are the Trusted Internet Connections (TIC) initiative, Federal Information Security Management Act (FISMA) implementation and oversight, development and deployment of EINSTEIN detection and prevention capabilities, Continuous Monitoring and Mitigation technologies, and the cyber incident response capabilities of the U.S. Computer Emergency Readiness Team (US-CERT). Most recently, he served as the Chief Information Officer (CIO) for the U.S. Department of Energy (DOE), where he was the principal information management advisor to the Secretary of Energy and the senior IT and cybersecurity official for the DOE. Mr. Locatis promoted Department-wide innovation and effective operations by engaging stakeholders across the entire DOE complex. Through collaboration with national laboratories, program executives, DOE Federal information management staff and contractors, external agency partners and strategic industry partners, he established strategy, policy, direction and a skilled workforce that best support DOE's mission and objectives. In recognition for his leadership Mr. Locatis was a recent recipient of the 2012 Federal 100 Award – recognizing him for the development of the DOE Joint Cybersecurity Coordination Center (JC3), which applies a proactive approach to risk management policy enterprise-wide and vastly improves situational awareness, incident management and cross-agency collaboration.

Lisa Lorenzin, Juniper Networks

Lisa Lorenzin is a Principal Solutions Architect with Juniper Networks, specializing in security and mobility solutions, and a contributing member of Trusted Network Connect, a work group of the Trusted Computing Group that defines an open architecture and standards for endpoint integrity and network security. She has worked in a variety of Internet-related roles since 1994, with more than a decade of that focused on network and information security, and is currently concentrating on enterprise security including security automation, network segmentation, end-to-end identity-based access control, and integration of mobile security.

Dave Marcus, McAfee Labs

Dave Marcus currently serves as Director of Advanced Research and Threat Intelligence for McAfee® Labs, focusing on bringing McAfee's extensive security research and global threat intelligence to McAfee's customers and the greater security community. With more than twelve years of technical experience in information security, network and host intrusion analysis and prevention, Mr. Marcus' current focus at McAfee Labs includes advanced research and threat intelligence projects such as Open Source Intelligence (OSINT) analysis, financial fraud malware, hardware-assisted security architecture and SCADA/ICS research. He is also co-host of Audio-Parasitics – The Official Podcast of McAfee Labs. Mr. Marcus also has responsibilities for all publications from McAfee Labs, such as the Labs' journal of security vision The McAfee Security Journal as well as its Quarterly Threat Report. In his spare time he collects guitars, is an avid powerlifter and is a founding keyholder of Unalocated Space, a Maryland Hackerspace. He also enjoys practicing the art of lockpicking and is a hacker of things.

Robert Martin, MITRE Corporation

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

Daniel Matthews, Information Innovators, Inc.

Mr. Matthews serves as the Executive Vice President for Health IT at Information Innovators, Inc. (Triple-i). Triple-i provides federal Health IT clients with information technology infrastructure services, strategic planning, information assurance and application development lifecycle support. Mr. Matthews advises the company on matters ranging from new business acquisitions to client relationship management. Mr. Matthews joined the Lockheed Martin Corporation as a computer programmer in 1978 at its Orlando facility. In 1983 he was appointed to the Director of Accounts for the Baltimore Aerospace Division and was later elevated to Director of the Dayton, OH, Information Technology program office. Dan returned to the Washington, DC area in 1991 and ran several program efforts throughout the company. From 1994 until 1998 Matthews served as Vice President of Civil Agency efforts of BDM International, which was later acquired by Northrop Grumman. In 2003, Mr. Matthews was selected for the Presidential appointment as Chief Information Officer (CIO) for the Department of Transportation. While serving as CIO for Transportation he was elected to the position of Vice Chair of the Federal CIO Council by his fellow CIO's. In 2006 he returned to Lockheed Martin as VP Washington Operations and retired in 2010. Matthews served in the United States Air Force, being honorably discharged in 1975. Dan holds a bachelor's degree in Management from Kent College and Master's of Science degree in Business Administration for Strayer University. Dan is also a 1991 graduate of the DoD Defense System Management College at Fort Belvoir, Virginia.

Tom Millar, DHS

Tom Millar serves as the United States Computer Emergency Readiness Team's (US-CERT) Chief of Communications, a role which finds him at the intersection of outreach, awareness, standards development, and technical interoperability initiatives. In this role, Mr. Millar is focused on modernizing US-CERT's approaches to information sharing, knowledge exchange and coordination. Since joining US-CERT in 2007, he has played a significant role in US-CERT's response activities during major cyber events such as the Distributed Denial of Service (DDoS) attacks on Estonia in 2007, the outbreak of the Conficker worm, and the DDoS attacks on major U.S. Government and commercial Web sites in 2009. Mr. Millar has previously worked as a team lead for intrusion detection and analysis at the FBI's Enterprise Security Operations Center. Prior to his cybersecurity career, he served as a linguist with the 22nd Intelligence Squadron of the United States Air Force. Mr. Millar has a Master's of Science in Engineering Management from the George Washington University.

George Moore, Department of Homeland Security

George Moore is technical director of the National Cyber Security Division at the Department of Homeland Security. Formerly, he worked on Cyber issues at USAID and the Department of State. George was a member of a Team that received an NSA Roulette Award for related work.

Dennis Moreau, RSA

Dennis is a Senior Technology Strategist in the Office of the CTO at RSA, specializing in Utility Computing Security and Advanced Threat Response technologies. Dennis has over than 35 years of experience in designing and implementing system management and security applications and infrastructures. Prior to joining RSA, Dennis was a founder and the Chief Technology Officer for Configuresoft, a compliance technology now in the VMWare portfolio. He was also the CTO for Baylor College of Medicine (BCM). He holds a doctorate in Computer Science and has held faculty positions in Computational Medicine and Computer Science.

Kathleen Moriarty, EMC Corporation

Kathleen 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.

Matthew Myrick, Senior Security Engineer, Lawrence Livermore National Laboratory

Matthew Myrick is a Senior Security Engineer and member of the Incident Response Team at Lawrence Livermore National Laboratory (LLNL). His research interests include network defense, incident response, reverse engineering, penetration testing and forensic analysis. He is a frequent speaker and advocate of computer security throughout the Department of Energy and Defense Industrial Base. He holds a Master of Science in Computer Science from California State University, Chico as well as a CISSP, GCIA, GPEN, BCCPA.

Alan Paller, SANS Institute

Alan Paller is director of research at the SANS Institute, a graduate degree granting institution and the principal cyber security training school. SANS' 115,000 alumni are technical security experts and managers holding responsible positions in cyber defense, offense, and law enforcement in more than 60 countries. Alan directs SANS research programs including the widely used Internet Storm Center - the early warning system for the Internet and the annual "Greatest Risks in Cyber Security" study. He also oversees NewsBites, the bi-weekly summary of the top news in security that goes to 210,000 people, and @RISK, and the weekly authoritative summary of all new vulnerabilities and all critical new vulnerabilities made known during the past week that goes to 120,000 people. Alan has testified several times before both the House and Senate and in 2001 President Clinton named him as one of the first members of the National Infrastructure Assurance Council. In 2005, the Federal CIO Council selected him as their annual Azimuth Award winner recognizing the one person outside government whose vision and leadership have done the most to improve federal information technology. In 2007, eWeek and Baseline magazines selected Alan as one of the 100 most important people in the information technology industry. Alan's degrees are from Cornell University and the Massachusetts Institute of Technology.

Speaker Biographies (continued)

Franklin Reeder, NBISE

Frank served at the U.S. Office of Management and Budget for two stints totaling more than 20 years between 1970 and 1995 where he was chief of Information Policy, Deputy Associate Director for Veterans Affairs and Personnel, and Assistant Director for General Management. While a member of the information policy staff and later as its chief, he represented the Administration in negotiating and securing enactment of the Privacy Act of 1974 and the Computer Security Act of 1987 and wrote the guidelines on implementing the Privacy Act. Also while at OMB he was the U.S. Delegate to the Organization for Economic Cooperation and Development's Public Management Committee (OECD/PUMA) from 1992-1995 and he chaired that committee from 1993-95. From 1995-97, he served as Director of the Office of Administration of the Executive Office of the President. From 2004-12 he served as a coach in the Council for Excellence in Government/Partnership for Public Service excellence in government leadership fellows program. He was a member of the Obama-Biden Presidential Transition Team serving on the OMB and White House agency review teams and the technology innovation and government reform team with particular emphasis on the performance and accountability agenda. He chaired the Information Security and Privacy Advisory Board from 1998 through 2004 and was a member of the Commission on Cyber Security for the 44th Presidency and of the Social Security Commissioner's advisory panel on Future Systems Technology from 2008 through 2012.

Andrew Rikarts, U.S. Dept of Veterans Affairs

Andrew Rikarts, Enterprise Visibility Program Manager at the U.S. Department of Veterans Affairs providing visibility and vulnerability management capability to over 700,000 endpoints with over 400,000 desktops, laptops and servers covered by BigFix. Andrew is on his eighth year with VA, having served as CIRC Manager and Enterprise Technical Security Officer. Andrew came to the VA after being part of the team that built security into the Navy's and Marine's Corps' Intranet while working for Raytheon, and prior to that, twelve years in the commercial world as an IT Manager and programmer in the Health and Life Insurance Industry.

Tim Ruland, US Census Bureau

Mr. Ruland began his career at the Census Bureau in 1991 when he was hired to establish a configuration management process for the 1992 Economic Census. After which he earned the position of Division Security Officer. After spending 18 months as the Division Security Officer, Configuration Manager and system administrator, Mr. Ruland moved to the ADP Security Branch. The ADP Security Branch was a small branch of seven people in the Administrative and Finance Division. In 1998, Mr. Ruland was promoted to Branch Chief where his first action was to change the name of the organization to better reflect the more diverse role of the organization, the IT Security Branch. Mr. Ruland has been instrumental in the development of the Census Bureau IT Security Program and the office has grown to four staffs consisting of 27 employees and approximately 20 contractors in support of the enterprise IT Security Program. He has managed the Census Bureau IT Security Program through two Decennial Census operations in 2000 and 2010 and is engaged in security planning for the 2020 Decennial Census. He has begun to implement the Risk Management Framework at the Census Bureau and began by deciding to completely change the process of system security to one that embraces and fosters a risk based environment. He and his team have briefed Ron Ross on the process and at Ron's suggestion have begun to present the Census Bureau framework methodology to other federal agencies. Mr. Ruland holds a Sociology Degree from the University of Maryland.

Roselle Safran, DHS/US-CERT

Roselle Safran has over 10 years of experience in technology fields. She is presently the Deputy Chief for Digital Analytics at the Department of Homeland Security's US-CERT where she manages various daily operations activities for the Forensic Analysis and Malware Analysis teams. She is also responsible for project management as the Product Owner for two information sharing software applications: an analysis collaboration platform utilized internally by US-CERT analysts and an information repository used by 50 Federal departments and agencies to exchange computer network defense knowledge. Ms. Safran's prior industry experience includes extensive work in computer forensics, incident response, electronic data collection and Internet investigations. She has handled cyber crime cases involving network intrusions, theft of intellectual property, software piracy, spamming activities, defamation, regulatory violations, and various types of fraud. Before entering the field of cyber investigations, Ms. Safran was an entrepreneur and founded, managed and then sold a web-based business. Ms. Safran holds a Bachelor of Science in Engineering degree from Princeton University.

Chris Salter, NSA

Chris Salter has worked for the NSA for over 20 years. He was trained as a cryptographer but now focuses on fostering commercial standards that will enable critical infrastructures to defend their data and systems from sophisticated adversaries.

Leo Scanlon, National Archives

Chief Information Security Officer at National Archives and Records Administration since 2005. As a security specialist with Northrup Grumman, lead a team that developed the FISMA certification for the IRS Modernized Infrastructure. Prior background as a specialist in physical and IT security in the telecommunications industry.

Charles Schmidt, The MITRE Corp.

Charles 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 Bachelors degree in both Mathematics and Computer Science from Carleton College and a Masters degree in Computer Science from the University of Utah.

Josh Shaul, Application Security, Inc.

As the Chief Technology Officer with Application Security, Inc. (AppSec), Josh Shaul is responsible for the overall direction of the organization's technical strategy, which includes responsibility for the product portfolio – AppDetectivePro for auditors and IT advisors, and its flagship solution, DbProtect for the enterprise. During his tenure at AppSec, Josh has held positions in product management, engineering, sales and technical strategy. Prior to AppSec, Josh was Director, Worldwide Systems Engineering with SafeNet, Inc. working on the industry's first complete IPsec accelerator chip. In his five years with SafeNet, he was responsible for the design, development and enhancement of SafeNet's embedded security solutions, covering a wide range of applications. He is the author of the acclaimed *Practical Oracle Security: Your Unauthorized Guide to Relational Database Security*, which received resoundingly positive critical reviews. He's presented at numerous global technology conferences including Microsoft TechEd, McAfee FOCUS, InfoSec World, WhiteHatWorld, Computer Security Institute, GFirst, IOUG COLLABORATE, several Oracle Users Group conferences, Federal Information Assurance Technology Forum, OWASP, Federal Information Security Conference, and FS-ISAC. Josh holds a B.S. in Computer Systems Engineering from the University of Massachusetts.

Verdis Spearman, U.S. Department of Homeland Security

Verdis Spearman serves as Team Lead for the United States Computer Emergency Readiness Team (US-CERT) Government Sector Coordination Program. He is responsible for increasing the quality of coordination and collaboration between US-CERT and Federal Departments and Agencies, State, Local, Territory and Tribal entities. Verdis has enjoyed a dynamic career as a project manager, system engineer, software developer, network administrator and security practitioner on Research and Development (R&D) projects at the Defense Advanced Research Projects Agency, the Defense Information Systems Agency and Defense Threat Reduction Agency (DTRA). Prior to arriving to DHS in July 2009, he was a Project Manager and Lead System Engineer at the DTRA Nuclear Technologies Directorate. He led the engineering team in developing and maintaining the computerized "Chemical, Biological, Nuclear, Radiological and Explosives" (CBNRE) effects modeling and simulation (M&S) system known as the "Integrated Weapons of Mass Destruction Toolset." In parallel, he led the system development and management of the DTRA Meteorological Data Service (MDS) platform. He additionally led the development team to integrate both platforms, which currently serves as the Nation's "de facto" CBNRE Consequence Management system. Verdis holds a Bachelor of Science degree in Internetworking Technology and Network Security from Strayer University.

Richard Spires, US Dept. of Homeland Security

Richard A. Spires was appointed in September 2009 to serve as the Chief Information Officer (CIO) of the Department of Homeland Security (DHS). He is responsible for the department's \$6.8 billion investment in Information Technology (IT). He leads and facilitates portfolio management, development, implementation, and maintenance of the department's IT architecture. Mr. Spires is the chairman of the DHS Chief Information Officer Council and the Enterprise Architecture Board. Mr. Spires serves on the Federal CIO Council, where he was selected vice chairman by its members in January 2011. He also serves as co-chair of the council's Federal Data Center Consolidation Task Force and previously co-chaired the Management Best Practices Committee. Mr. Spires held several positions at the Internal Revenue Service (IRS) from 2004 through 2008. He served as the Deputy Commissioner for Operations Support, having overall responsibility for the key support and administrative functions for the IRS, including IT, Human Capital, Finance, Shared Services, Real Estate, and Security functions. Before becoming Deputy Commissioner, Mr. Spires served as CIO of the IRS, with overall strategic and operational responsibility for a \$2 billion budget and a 7,000-person Modernization and Information Technology Services organization, being accountable for maintaining more than 400 systems administering in excess of 200 million taxpayer records and supporting more than 100,000 IRS employees. Mr. Spires served for two and half years as the Associate CIO for Applications Development and led the IRS's Business Systems Modernization program, one of the largest and most complex information technology modernization efforts undertaken to date. From 2000 through 2003, Mr. Spires served as President, Chief Operating Officer, and Director of Mantas, Inc., a software company that provides business intelligence solutions to the financial services industry. In helping to establish Mantas, Mr. Spires successfully led efforts to raise \$29 million in venture funding. Before Mantas, Mr. Spires spent more than 16 years serving in a number of technical and managerial positions at SRA International. Mr. Spires received a B.S. in Electrical Engineering and a B.A. in Mathematical Sciences from the University of Cincinnati. He also holds an M.S. in Electrical Engineering from the George Washington University. Mr. Spires was named Distinguished Alumnus by the University of Cincinnati's College of Engineering in 2006.

Elayne Starkey, State of Delaware

Elayne Starkey is the Chief Security Officer for the State of Delaware/Department of Technology and Information (DTI) and responsible for the enterprise-wide protection of information assets from high consequence events, including cyber and physical terrorism, and natural disasters. Elayne is the Chair of the Delaware Information Security Officer Team and member of the Governor's Homeland Security Council. She has been a member of the Multi-State Information Sharing and Analysis Center (MS-ISAC) since its inception in 2003. She serves on the MS-ISAC Executive Board and a past co-chair of the Education and Awareness work group. Elayne is also a member of National Association of Chief Information Officers (NASCIO) Security and Privacy Committee, and the Information Systems Security Association (ISSA). In 2012, Elayne was honored as one of 10 most Influential People in Government Information Security, and in 2011 was a Computer Week's Federal 100 winner. Elayne was previously the Chief Technology Officer at DTI and the Chief Information Officer for the Delaware Department of Public Safety. Prior to joining state government, Elayne spent 12 years in the private sector in software engineering roles at Xerox Corporation in Rochester, NY and Perdue Farms Inc., in Salisbury, MD. Elayne holds a Bachelors of Science degree in computer science, math, and business administration from James Madison University and a Master's degree in Computer Science from Rochester Institute of Technology with concentrations in Software Engineering and Data Communications.

Speaker Biographies (continued)

John Streufert, Dept. of Homeland Security

In 2012 John Streufert joined the U.S. Department of Homeland Security (DHS) as the Director of the National Cyber Security Division. In this role, he leads DHS's effort to build and maintain an effective national cyberspace response system and to implement a cyber risk management program in the form of continuous monitoring, diagnosis and mitigation. Between 2006 and 2012, Mr. Streufert served as the Department of State's Chief Information Security Officer and the Deputy Chief Information Officer for Information Assurance. In July 2008, at Mr. Streufert's request, the State Department began using monthly letter grades to measure executive and technical managers' progress reducing the risk posed to their IT systems. His earlier federal assignments were with the US Agency for International Development, the Department of Agriculture and the Department of Navy.

Tony Summerlin, TA Summerlin

Tony Summerlin has more than 25 years of experience and has been a huge force behind the scenes supporting the Federal CIO, the CIO Council, and E-Gov Program Managers. In 2009 he was awarded his second Fed 100 for his support of the Presidential Transition and his dedication to the Federal E-Government Program. Mr. Summerlin has worked tirelessly for almost a decade to achieve the goals of the E-Gov Act. Before Co-Founding Kickstand Mr. Summerlin led the Touchstone Consulting Group, developing E-Gov programs for many Federal Agencies. In addition to his intimate involvement with the E-Government work in the Federal Government Mr. Summerlin also served as a E-Government advisor to the government of Mexico. During Project Quicksilver Mr. Summerlin created and implemented the Program Management Office at OMB to effectively manage the first generation of 25 E-Gov initiatives. He is presently serving the Congressionally formed Commission for Research and Development for the Director of National Intelligence as the lead on Cyber related issues. He holds two technology patents and is the co-author of two leading academic titles.

James Tarala, Enclave Security

James Tarala is a principal consultant with Enclave Security and is based out of Venice, Florida. He is a regular speaker and senior instructor with the SANS Institute as well as a courseware author and editor for many SANS auditing and security courses. As a consultant, he has spent the past few years architecting large enterprise IT security and infrastructure architectures, specifically working with many Microsoft-based directory services, e-mail, terminal services, and wireless technologies. He has also spent a large amount of time consulting with organizations to assist them in their security management, operational practices, and regulatory compliance issues, and he often times performs independent security audits and assists internal audit groups to develop their internal audit programs. James completed his undergraduate studies at Philadelphia Biblical University and his graduate work at the University of Maryland. He holds numerous professional certifications.

Gil Vega, Dept. of Energy

As the Associate Chief Information Officer for Cybersecurity, Mr. Vega serves as the Department of Energy's Chief Information Security Officer (CISO) charged with leading the agency's enterprise cybersecurity program. Mr. Vega advises the Department's CIO and senior agency officials in the implementation of cybersecurity and the Department's Risk Management Approach. Mr. Vega provides executive leadership and guidance for joint agency and Administration cybersecurity initiatives including for the Comprehensive National Cybersecurity Initiative, safeguarding of the Defense Industrial Base, supporting the Department's cybersecurity R&D programs and critical infrastructure protection. Mr. Vega is a career member of the Senior Executive Service. Prior to joining the Department, Mr. Vega served as the CISO & IT Risk Executive for U.S. Immigration & Customs Enforcement (ICE), the largest investigative agency within the U.S. Department of Homeland Security (DHS). While at ICE, Mr. Vega built a transformative, award-winning cybersecurity program to better enable the law enforcement mission of ICE and its partners. By embracing a true risk-based approach, ICE's cybersecurity program enhanced the tactical and data sharing capabilities for DHS and its stakeholder community. These efforts culminated in unprecedented success in counter-terrorism information sharing with foreign governments and leading-edge security infrastructure modernization. Mr. Vega is a Certified Information Systems Security Professional and has a Bachelor of Science in Computer Information Systems and graduated with a Master of Science degree in Information Assurance from Norwich University. Mr. Vega is also a graduate of the Federal Executive Institute in Charlottesville, Virginia and a veteran of the United States Army, where he participated in combat operations in Saudi Arabia/Kuwait/Iraq (Operations Desert Shield/Storm).

Kimberly Watson, NSA/IAD, Technical Director, Analysis and Data Fusion Group; Fusion, Analysis, and Mitigations Deputy Directorate; Information Assurance Directorate; National Security Agency

Ms. Kim Watson is has been at NSA for more than 25 years, most of which has been spent in FAM or one of its predecessor organizations (i.e., some type of vulnerability discovery or technology evaluation activity). For the last 9 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.

Eric Winterton, Booz Allen Hamilton

Eric Winterton, CISSP, is the Director of the Cyber Assurance Testing Laboratory at Booz Allen Hamilton and has more than 20 years of 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 holds an undergraduate degree in computer science and a Master's Degree in Technical Management from Johns Hopkins University.

Greg Witte, G2, Inc

Greg Witte leads the U.S. Federal civilian team at G2, Inc., and works closely with NIST and DHS to improve risk management through security data integration and automation.

Lisa Young, CERT Carnegie Mellon University

Lisa Young is a senior member of the technical staff at CERT in the Software Engineering Institute at Carnegie Mellon University where she serves as a contributing developer of the Resilience Management Model (RMM) and the Appraisal Team lead. Young holds the designation of Certified Information Systems Auditor (CISA), Certified Information Security Manager (CISM), Certified Information Systems Security Professional (CISSP) and is experienced in IT governance, audit, security and risk management. Lisa teaches the Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE®) risk-based assessment methodology at the Software Engineering Institute. Young was a member of the ISACA international task force that developed the RISK-IT Framework and Practitioner's guide, a risk framework based on COBIT® which provides guidance for organizations in managing IT-related business risks.

Wes Young, REN-ISAC

Wes Young is the Principal Security Architect of the Research and Education Networking Information Sharing and Analysis Center (REN-ISAC). Information about his current project can be found at collectiveintel.net.

Vendor Information



Agilience www.agilience.com

Agilience is the leading independent provider of Security Risk Management solutions. Agilience RiskVision is automating how Global 2000 companies and government agencies achieve continuous monitoring of big data across financial, operations, and IT domains to orchestrate incident, threat, and vulnerability actions in real time. Agilience RiskVision scales with businesses, effectively managing assets, data, people, and processes to achieve 100 percent risk and compliance coverage.



Application Security, Inc. www.appsecinc.com

Application Security, Inc. (AppSecInc) is a pioneer and leading provider of database security and compliance solutions for the enterprise. By providing strategic and scalable software-only solutions, AppDetectivePro for auditors & IT advisors, and DbProtect for the enterprise, AppSecInc supports the database lifecycle for some of the most complex & demanding environments in the world. AppSecInc products leverage the knowledgebase from their renowned team of threat researchers, Team SHATTER, for unprecedented levels of data security.



HP Enterprise Security www.hpenterprisesecurity.com

HP is a leading provider of security and compliance solutions for modern enterprises that want to mitigate risk in their hybrid environments and defend against advanced threats. Based on market leading products from ArcSight, Fortify, and TippingPoint, the HP Security Intelligence and Risk Management (SIRM) Platform uniquely delivers the advanced correlation, application protection, and network defense technology to protect today's applications and IT infrastructures from sophisticated cyber threats.



Intel premierit.intel.com/community/ipip/fedgov

Intel's mission is to create and extend computing technology to connect and enrich the lives of every person on earth. As the world's largest semiconductor chip maker, we develop advanced integrated digital technologies, primarily integrated circuits, for industries such as computing and communications. Intel is transforming from a company with a primary focus on the design and manufacture of chips for PCs and servers to a computing company that delivers complete solutions in the form of hardware and software platforms and supporting services. Our goal is to be the preeminent computing solutions company that powers the worldwide digital economy. Intel also works with governments, organizations, and industries around the world to advocate policies that encourage new ideas, promote fair commerce, and protect resources. By promoting innovation and competition worldwide, Intel seeks to help people, government and businesses thrive in an increasingly global economy. Connect with the Intel Premier IT Professional Federal Government community at Premierit.intel.com/fedgov or email us at federal@intel.com.



Lunarline, Inc. www.lunarline.com

Lunarline is a leading cyber security and privacy provider to the US Federal Government, as well as private industry. Our unique approach to cyber security combines our proven products, specialized services, and certified training together as a complete solution customized for the success of your cyber mission. Our solutions are designed around the concept of security automation and flexible integration with other tools. We understand that these principles are driving the future of cyber security and continuous monitoring. Lunarline is an accredited FedRAMP Third Party Assessment Organization (3PAO).



Mitre <http://makingsecuritymeasurable.mitre.org/about/index.html>

MITRE's "Making Security Measurable" effort provides building blocks for transforming cybersecurity. Through standard enumerations and languages, information amongst tools and organizations can dramatically change your security posture, vendor independence and flexibility. Visit our booth for more about these community efforts: CVE, CCE, CPE, CAPEC, CWE, CEE, MAEC, CybOX, STIX, and OVAL.



n circle www.ncircle.com

nCircle is the leading provider of Information Risk & Security Performance Management solutions to more than 6,500 businesses and government agencies worldwide. nCircle solutions enable enterprises of all sizes to 1) automate compliance and reduce risk, and 2) measure and compare the performance of their IT security program with their own goals and industry peers. nCircle solutions may be deployed on a customer's premise, as a cloud-based service, or in combination, for maximum flexibility and value. www.ncircle.com

Vendor Information (continued)



National Security Agency www.nsa.gov

The Information Assurance Directorate (IAD) delivers mission enhancing information assurance technologies, products and services that enable customers and clients to secure operational information and information systems.



NetIQ www.netiq.com

NetIQ Corporation is an enterprise software company with a relentless focus on delivering customer success. Our portfolio includes award-winning software solutions for identity, access, security, compliance, systems, application, and resource management. We help organizations securely deliver, measure, and manage computing services across physical, virtual, and cloud computing environments with an emphasis on reducing cost, complexity, and risk in highly distributed application environments.



NIST <http://csrc.nist.gov/nccoe>

The National Cybersecurity Center of Excellence (NCCoE) is a public-private collaboration that brings together experts from industry, government, and academia to design, implement, test, and demonstrate integrated cybersecurity solutions and promote their widespread adoption. Participants develop practical, interoperable cybersecurity approaches that address the real-world needs of complex information technology (IT) systems. Through research, development, and deployment acceleration efforts, the center:

- enhances trust in U.S. IT communications, data, and storage systems;
- lowers risk for companies and individuals using IT systems; and
- encourages development of innovative, job-creating cybersecurity products and services.

The center is hosted by the U.S. Commerce Department's National Institute of Standards and Technology (NIST) in collaboration with the State of Maryland and Montgomery County, Md.



Qualys, Inc. www.qualys.com

Qualys, Inc., is a pioneer and leading provider of cloud security and compliance solutions with over 5,800 customers in more than 100 countries, including a majority of each of the Forbes Global 100 and Fortune 100. The QualysGuard Cloud Platform and integrated suite of solutions helps organizations simplify security operations and lower the cost of compliance by delivering critical security intelligence on demand and automating the full spectrum of auditing, compliance and protection for IT systems and web applications. Founded in 1999, Qualys has established strategic partnerships with leading managed service providers and consulting organizations including BT, Dell SecureWorks, Fujitsu, IBM, NTT, Symantec, Verizon, and Wipro. The company is also a founding member of the Cloud Security Alliance (CSA). For more information, please visit www.qualys.com.



RSA www.rsa.com

RSA, The Security Division of EMC, is the premier provider of security, risk and compliance management solutions for business acceleration. RSA helps the world's leading organizations solve their most complex and sensitive security challenges. These challenges include managing organizational risk, safeguarding mobile access and collaboration, proving compliance, and securing virtual and cloud environments. Combining business-critical controls in identity assurance, encryption & key management, SIEM, Data Loss Prevention, Continuous Network Monitoring, and Fraud Protection with industry leading eGRC capabilities and robust consulting services, RSA brings visibility and trust to millions of user identities, the transactions that they perform and the data that is generated. For more information, please visit www.RSA.com and www.EMC.com.



Symantec www.symantec.com/publicsector_us

Symantec is a global leader in providing security, storage and systems management solutions to help our customers – from consumers and small businesses to the largest global organizations – secure and manage their information-driven world against more risks at more points, more completely and efficiently. As the world's fourth largest independent software company, our unique focus is to eliminate risks to information, technology and processes independent of device, platform, interaction or location. Our software and services protect completely, in ways that can be managed easily and with controls that can be enforced automatically – enabling confidence wherever information is used or stored.

Vendor Information (continued)



Threat Guard www.threatguard.com

ThreatGuard, Inc. is a privately held, independent technology developer dedicated to producing innovative products for network security.



Trend Micro www.trendmicro.com/us/index.html

Trend Micro Incorporated, a global cloud security leader, creates a world safe for exchanging digital information with its Internet content security and threat management solutions for organizations and consumers. A pioneer in server security with over 20 years' experience, we deliver top-ranked client, server and cloud-based security that fits our customers' and partners' needs, stops new threats faster, and protects data in physical, virtualized and cloud environments. Powered by the industry-leading Trend Micro™ Smart Protection Network™ cloud computing security infrastructure, our products and services stop threats where they emerge - from the Internet. For more information, see www.TrendMicro.com.



Trusted Computing Group www.trustedcomputinggroup.org

The Trusted Computing Group (TCG) is a not-for-profit organization formed to develop, define and promote open, vendor-neutral, global industry standards, supportive of a hardware-based root of trust, for interoperable trusted computing platforms.



Websense www.websense.com

Websense, Inc., the global leader in integrated Web, data and email security solutions, provides Essential Information Protection™ for organizations worldwide. Distributed through its network of channel partners, Websense software and hosted security solutions help organizations block malicious code, prevent the loss of confidential information and enforce Internet use and security policies.

www.websense.com

SECURE & HARDEN YOUR DATA. ACHIEVE COMPLIANCE.

DbProtect Precision Database Activity Monitoring Solution



Visit **Booth 29** to see for yourself how you can secure your databases and achieve compliance.

Get a **free demo** of DbProtect.

Join AppSecInc CTO Josh Shaul's Solution Track Presentation: "Hacking Databases: Exploiting The Top Database Vulnerabilities And Misconfigurations"
Wednesday, October 3rd, 1145AM

**APPLICATION
SECURITY, INC.**
Effective Database Defense

350 MADISON AVENUE, 6TH FLOOR, NEW YORK, NY 10017 TOLL FREE 866 9APPSEC MAIN +1 212 912 4100 FAX +1 212 947 8788

The QualysGuard Cloud Platform

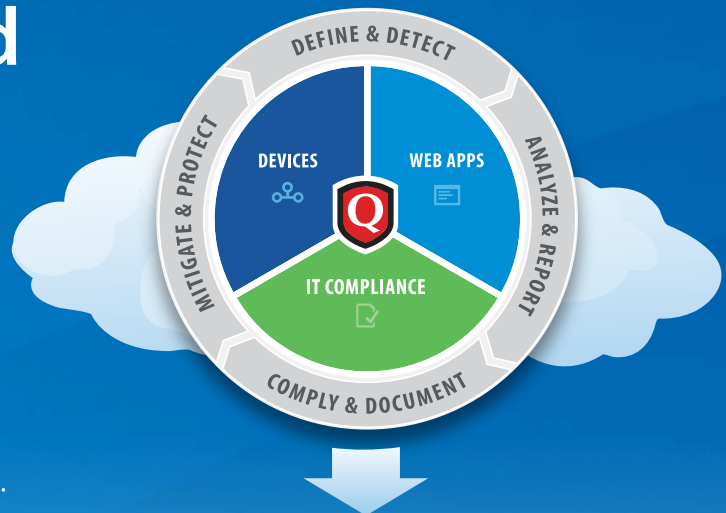
A Unified View of Your Security & Compliance

The QualysGuard Cloud Platform is used by over 5,800 organizations in more than 100 countries, including more than 50 of the Forbes Global 100.

Try our on demand services at qualys.com/trials



© 2012 Qualys, Inc. All rights reserved.



Actionable Security Intelligence



Vulnerabilities



Malware



Compliance

CAN YOU SEE EVERYTHING AT ONCE?

YOU CAN.

You can't stop threats if you can't spot them. That's why HP Enterprise Security offers proven solutions that deliver context-aware visibility into security risk. There's no better way to proactively detect security issues and drive situational awareness across your applications, operations, and infrastructure. The HP Security Intelligence and Risk Management platform provides integrated correlation, application protection and network defenses that can secure modern IT environments from sophisticated threats.

For more information go to
www.hpenterprisesecurity.com.

Advanced protection against
advanced threats.



Copyright © 2011 Hewlett-Packard Development Company, L.P.



ENTERPRISE SECURITY

SECURITY: You can get there from here

Together, Intel and McAfee deliver security for your entire enterprise, with built-in technology for non-stop trusted computing.

Contact your Intel advisor today at Federal@intel.com



Want to know more?



¹ Intel® Virtualization Technology requires a computer system with an enabled Intel® processor, BIOS, virtual machine monitor (VMM). Functionality, performance or other benefits will vary depending on hardware and software configurations. Software applications may not be compatible with all operating systems. Consult your PC manufacturer. For more information, visit <http://www.intel.com/go/virtualization>.

² No system can provide absolute security under all conditions. Requires an enabled chipset, BIOS, firmware and software and a subscription with a capable Service Provider. Consult your system manufacturer and Service Provider for availability and functionality. Intel assumes no liability for lost or stolen data and/or systems or any other damages resulting thereof. For more information, visit <http://www.intel.com/go/anti-theft>. 3 Intel® AES-NI requires a computer system with an AES-NI enabled processor, as well as non-Intel software to execute the instructions in the correct sequence. AES-NI is available on Intel® Core™ i5-600 Desktop Processor Series, Intel® Core™ i7-600 Mobile Processor Series, and Intel® Core™ i5-500 Mobile Processor Series. For availability, consult your reseller or system manufacturer. For more information, see <http://software.intel.com/en-us/articles/intel-advanced-encryption-standard-instructions-aes-ni/>.

⁴ Intel® vPro™ Technology is sophisticated and requires setup and activation. Availability of features and results will depend upon the setup and configuration of your hardware, software and IT environment. To learn more visit <http://www.intel.com/technology/vpro>.

⁵ KVM Remote Control (Keyboard, Video, Mouse) is only available with Intel® Core™ i5 vPro™ and Core™ i7 vPro™ processors with Intel® Active Management technology activated and configured and with integrated graphics active. Discrete graphics are not supported.

⁶ No computer system can provide absolute security under all conditions. Intel® Trusted Execution Technology (Intel® TXT) requires a computer system with Intel® Virtualization Technology, an Intel TXT-enabled processor, chipset, BIOS, Authenticated Code Modules and an Intel TXT-compatible measured launched environment (MLE). Intel TXT also requires the system to contain a TPM v1.s. For more information, visit <http://www.intel.com/technology/security>.

⁷ Requires activation and a system with a corporate network connection, an Intel® AMT-enabled chipset, network hardware and software. For notebooks, Intel AMT may be unavailable or limited over a host OS-based VPN, when connecting wirelessly, on battery power, sleeping, hibernating or powered off. Results dependent upon hardware, setup & configuration. For more information, visit <http://www.intel.com/technology/platform-technology/intel-amt>.

Copyright © 2012 Intel Corporation. All rights reserved. Intel, the Intel logo, vPro, Xeon, Ultrabook, Core inside, and Xeon inside are trademarks of Intel Corporation in the U.S. and other countries.

Copyright © 2012 McAfee, Inc. All rights reserved. McAfee, the McAfee logo, ePO, Total Protection, and DeepSAFE are trademarks or registered trademarks of McAfee, Inc.

*Other names and brands may be claimed as the property of others.

Defense against Threats with NetIQ



Securing data and systems requires continuous monitoring for detection of threats. NetIQ® Sentinel™ provides real-time visibility of events in your environment for disruption of threats before they can cause damage.

Here are a few of the solutions we plan to show you:

- Faster threat detection and remediation
- Easy configuration and adaptability
- Greater visibility into user activities
- Plug and play deployment

The U.S. Navy Cyber Defense Operations Command uses NetIQ Sentinel to prioritize security events, providing focus on those that require the most attention and ability to immediately act on what is most critical. NetIQ Sentinel is helping the U.S. Navy defend its networks 24/7 against persistent and adaptive threats.

Stop by **Booth 5** to learn how NetIQ solutions can help you secure mission-critical systems and data – and defend against damaging treats in your environment.



NEW DEFENSE STRATEGIES FOR ADVANCED THREATS



Lunarline is a leading and award winning provider of cyber security solutions, specialized Information Assurance services, and certified cyber security training to all US Federal Government (Civilian, DoD, and IC), as well as to customers in selected commercial markets. We believe in continuously improving our customer's ability to monitor and improve the confidentiality, integrity, and availability of their systems and applications.

All of Lunarline's solutions, services, and training are backed by our unwavering commitment to our customer's satisfaction, being a leader in cyber security innovation, while maintaining the highest quality standards.



Lunarline, Inc. | 3300 N. Fairfax Drive, Arlington, VA 22201
www.lunarline.com | call 571.481.9300 | email bizdev@lunarline.com

Your Continuous Monitoring Puzzle **Solved**



Agilience[®]
Managing Risk in Real Time

Visit Booth #36



A history of SCAP firsts.
... and we're just getting started.

Introducing




Your Compliance Multi-tool

- Continuous Monitoring
- Online & Offline Assessments
- Mobile or Fixed Deployment
- Assess MDM Systems
- Flexible Reporting
- Replay Target History
- Policy Deviation Management
- Much more...

www.threatguard.com

nCircle Information Risk & Security Performance Management


nCircle PureCloud™



Cloud-based Vulnerability Scanning
It's not hardware, it's not software,
it's PureCloud™

purecloud.ncircle.com

nCircle Suite360™




**Comprehensive Scanning
Delivering Actionable Intelligence**

- Vulnerability Management
- Web Application Scanning
- Certified PCI Scanning
- Configuration Auditing
- File Integrity Monitoring
- Reporting & Analytics

suite360.ncircle.com

nCircle Benchmark



Security Performance Management
Security Performance Metrics,
Scorecards & Industry Benchmarks

benchmark.ncircle.com



Secure your data against
targeted attacks.

Physical, Virtual or Cloud.

Analyst and security experts agree that risk management practices need to expand to deal with today's sophisticated attacks. Trend Micro continues to lead the way with the most comprehensive suite of security solutions for the public sector. **Join the Journey.**

Learn more at trendmicro.com/publicsector.

© 2012 Trend Micro, Inc. All rights reserved. Trend Micro and the T-ball logo are trademarks or registered trademarks of Trend Micro, Inc.

JOIN THE
JOURNEY

Architecting Measurable and Manageable Cyber Security

<http://makingsecuritymeasurable.mitre.org/>

Learn more at booth 23

MITRE

Making
Security
Measurable™



Protecting the world's information.

Cloud. Virtual. Mobile.

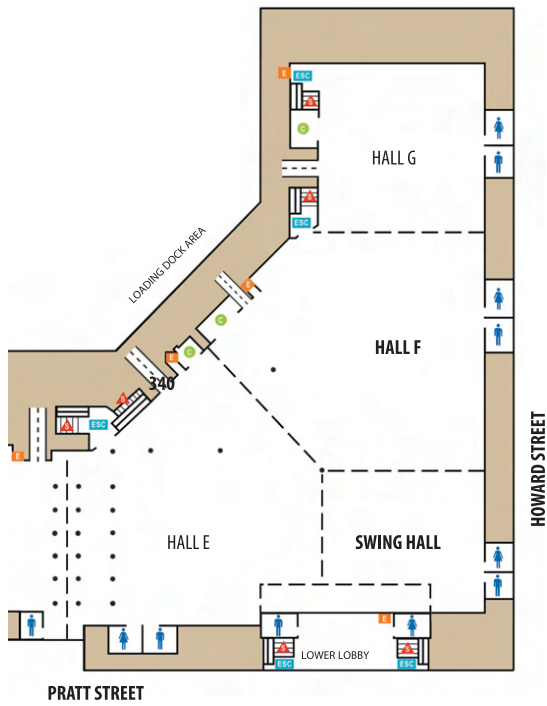


Today, we have more information than ever before and more ways to access it, process it, share it, and benefit from it. From tablets to cloud computing, from smartphones to virtualized data centers, from helping you defend your organization against advanced threats and data leaks to simplifying backup and ensuring 24x7 availability, Symantec helps protect your information no matter where it resides. **Visit Symantec at Booth #37.**

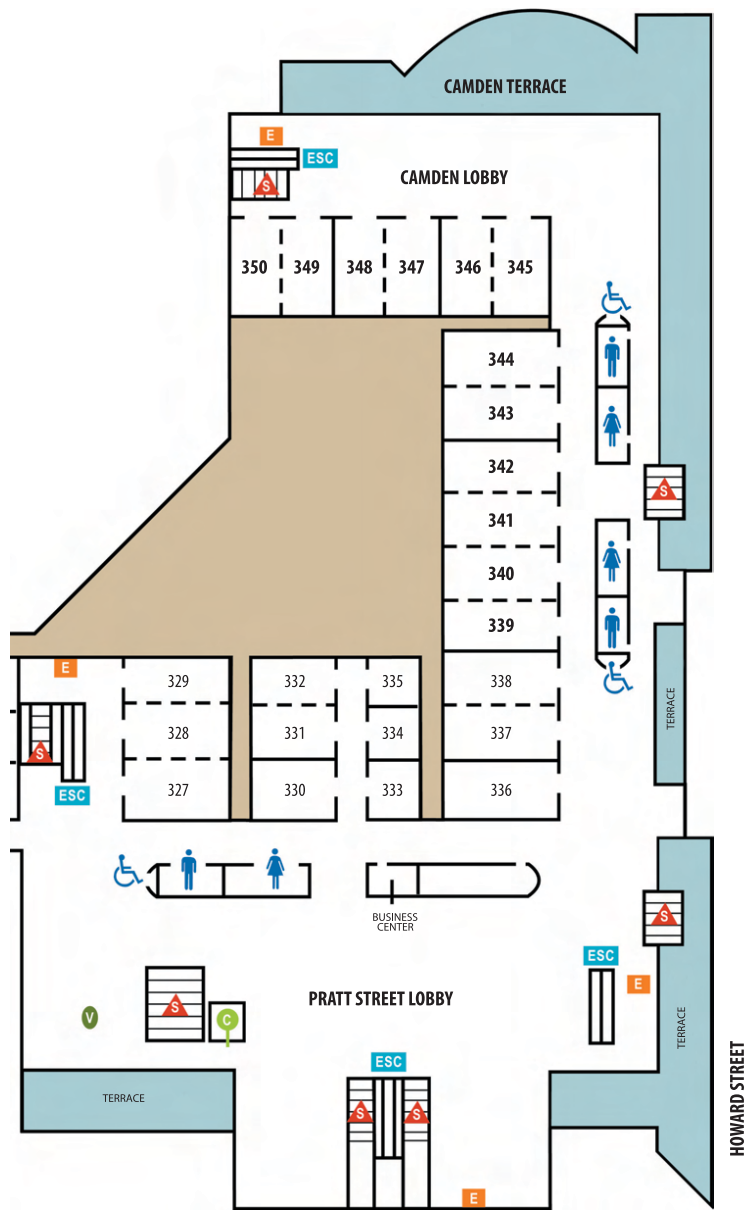


Convention Center Floorplan

LEVEL 100



LEVEL 300



LEVEL 400

