fissea
Federal Information Systems Security Educators' Association
AWARENESS • TRAINING • EDUCATION

"Making Connections in Cybersecurity and Information Security Education"
26th Annual Conference

Program updated 25Mar2013

Conference presentations will be posted to the FISSEA website, http://csrc.nist.gov/fissea

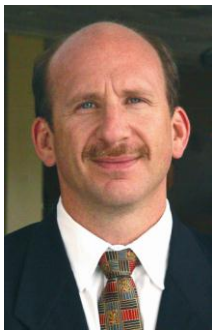
Tuesday, March 19, 2013

8:00 – 8:55 am	Registration, Breakfast, and Networking
9:00 – 9:15 am	**Conference Welcome**: Patricia Toth, NIST, FISSEA Conference Director **NIST Welcome:** Matthew Scholl, NIST Deputy Chief, Computer Security Division
9:15 – 10:00 am	**Keynote: Empowering Our Organizational Culture to Meet Today's Cybersecurity Challenges** Mr. John J. Suess, VP of IT & CIO, University of Maryland, Baltimore County (UMBC)

Empowering Our Organizational Culture to Meet Today's Cybersecurity Challenges

Cybersecurity has often been viewed as an IT initiative and is often focused narrowly on a small percentage of the individuals In an organization. As new threats emerge, such as social engineering, to broadly target individuals we need new approaches to address the challenge of cybersecurity. Broadly speaking, we need an approach that looks at cybersecurity holistically and builds support for a multi-year approach that incorporates better technology, new business processes, and an emphasis on communicating and educating workers. This approach requires leadership commitment to a long-term strategy for change management and organizational development around cybersecurity.

This talk will focus on ideas for effective change management and organizational development that are coupled with strategies for cybersecurity education, information sharing, and support to create long-term success. The talk will look at approaches used in other fields to change behavior and beliefs that could be used as models to build support for the change necessary to dramatically improve cybersecurity in our organizations. I will draw on approaches being developed in the higher education sector as well as lessons learned that can be applied to other groups.



Mr. Jack J. Suess, VP of IT & CIO, University of Maryland, Baltimore County (UMBC)

Jack Suess is Vice President for Information Technology and CIO at University of Maryland, Baltimore County (UMBC). He presently serves on the Internet2 Board of Directors; chairs InCommon Trust Services; chairs the advisory group for the Research & Education Network Information Sharing and Analysis Center (REN-ISAC; is past chair of the EDUCAUSE Higher Education Information Security Council;; and serves on the Management Council for the National Strategy for Trusted Identity in Cyberspace IDecosystem. More information is available at http://umbc.edu/~jack.

	TRACK 1: Green Auditorium
10:00 – 10:15 am	Morning Networking Break
10:15 – 11:00 am	**How to Use the National Cybersecurity Workforce Framework: Your Implementation Guide** Margaret "Peggy" Maxson, Department of Homeland Security

How to Use the National Cybersecurity Workforce Framework: Your Implementation Guide

In response to the need to define the cybersecurity workforce, an effort began in 2010 to establish a framework to categorize the work done by cybersecurity professionals. These efforts evolved as more than 20 Federal departments and agencies contributed to the process. The result was the development of the National Cybersecurity Workforce Framework (the Framework) by the National Initiative for Cybersecurity Education (NICE). The Framework was published in August 2012.

The purpose of the Framework is to establish a national standard to describe cybersecurity work irrespective of organizational structures, job titles, or other conventions. In designing the Framework, "categories" and "specialty areas" were used as an organizing construct to group similar types of work. The categories, serving as an overarching structure for the Framework, group related specialty

areas together. Within each specialty area, typical tasks and knowledge, skills, and abilities (KSAs) are provided.

To assist organizations with interpreting the Framework, NICE developed an interactive Implementation How-To Guide with instructions detailing how organizations can adopt the Framework. The How-To Guide provides information on Framework characteristics, the benefits of its use, and specific steps to apply the Framework into strategic human capital activities – including role definition, competency models and workforce planning. The How-To Guide assists in organizational adoption of the Framework, helping Academia, Government and Industry incorporate the Framework's specialty areas into its own Human Resource.

Discussions will include examples of how organizations are already adopting the Framework and how processes might be developed that can be used to encourage adoption.

Margaret "Peggy" Maxson, Director, National Cybersecurity Education Strategy
Department of Homeland Security (DHS) National Cybersecurity Education Office (CEO)

On April 19, 2010, Ms. Maxson was appointed to her position as Director of National Cybersecurity Education Strategy at the Department of Homeland Security. In this capacity, she leads DHS efforts to build capability within the National Initiative for Cybersecurity Education (NICE) as well as co-leads the training and professional development component of the initiative. DHS requested Ms. Maxson for this position following her previous position at the Office of the Director of National Intelligence, when she led a cybersecurity education sub-group of the White House, which resulted in the accepted recommendation and subsequent implementation of the establishment of NICE. Ms. Maxson served for over 35 years at the National Security Agency in managerial positions in operations, policy, foreign relations, customer service, and technology development.

	TRACK 1: Green Auditorium
11:05 – 11:40 am	**How to Plan for Your Cybersecurity Workforce** Robin "Montana" Williams, Department of Homeland Security

How to Plan for Your Cybersecurity Workforce

Do you know how to plan for the needs of your cybersecurity workforce? Do you know where to start? The need for cybersecurity specialists is increasing exponentially, and there are not enough professionals to meet the growing demand. Most organizations are not able to develop and train enough cybersecurity professionals to keep pace with that demand. Deliberate workforce planning addresses this and helps close the workforce gap in a systematic way. Using best practices, accurate workforce planning identifies skills and proficiency gaps across all cybersecurity roles. Join the National Initiative for Cybersecurity Education (NICE) in this session to hear about the best practices in cybersecurity workforce planning across Federal, State, and Industry organizations, as well as resources NICE has to help you improve future planning.

Robin "Montana" Williams, Director, National Cybersecurity Education Office (CEO) Director
National Cybersecurity Education Office (CEO)

Robin "Montana" Williams is currently the Director, National Cybersecurity Education & Workforce Development Office, Department of Homeland Security, Washington, D.C. His office is responsible for development of national cybersecurity education, policy, standards, and assessment requirements to broaden, develop, and maintain an unrivaled, globally competitive cybersecurity workforce for the nation. Additionally, his team executes two components of the 44th President's National Initiative for Cybersecurity Education (NICE). Prior, Mr. Williams served as a Senior Technical Program Manager for the National Counterintelligence Executive directing cyber counterintelligence training & threat analysis. Mr. Williams has spent 23 years in government service including 21 years in the United States Air Force retiring as a Lt. Colonel. During his military, he held numerous flying, intelligence, training, and cyberspace assignments, including commanding the USAF Cyber Red Team. He is a combat veteran with flying & information operations duties in Afghanistan and Iraq, including serving as the lead planner for OPERATION ANACONDA & Chief, Electronic Warfare in the Iraqi Theater of Operations. Mr. Williams earned a Bachelor's degree from Minnesota State University-Moorhead in 1989, a Master's degree from Louisiana Tech in 1998, and current completing a doctorate program. In addition, Mr. Williams is a Certified Workforce Development Professional.

	TRACK 1: Green Auditorium Daily Announcers: Track 1: Louis Numkin	**Track 2: Lecture Room B** MC: Art Chantker, Potomac Forum
11:45 - 12:15 pm	**Phishing – Are You Getting Hooked?** Janet Wilson and Michael Webber, C^2 Technologies	**Hiring and Managing a Cyber Security Workforce: What Federal Managers Need to Know** Scott Cameron, R3 Government Solutions, LLC

Phishing – Are You Getting Hooked?

This session discusses cases that focus on phishing attacks within the U.S. Government and other organizations. Phishing and social engineering are not new phenomena, but are growing in number due to the increased connectivity brought about by increasingly sophisticated mobile devices. The presentation will include case studies and profiles of present-day attack techniques, and will discuss the need to educate users continually to protect themselves and their organizations.

Profiles of a Present-Day Attack
Attackers use simple tools to profile organizations and look directly for vulnerabilities or for information about employees. Tools that will be discussed include:

- Maltego – An automated open source intelligence-gathering tool
- Social Engineering Toolkit (SCT)
- Spoof APP
- Social networking sites such as LinkedIn

Case Studies
Case 1: Not All Threats Are External
Jeffrey Dulal took classified information from the U.S. Navy. He didn't email the information, upload the information, or use a USB. All of these options had been disabled. He used a floppy disk.

Bradley Manning didn't use a floppy disk or USB. He used a CD disguised with a label of Lady Gaga. Observers' presumption was that the CD contained music, but Manning was leaving each day with classified information.

Case 2: Open Source Intelligence-Gathering
This involved a civil case in which the CFO of an international firm posted on a social media site that she had purchased a very nice high-end Nikon digital camera. The CFO received an email with a PDF attached that purported to be the latest manual for the camera. The email didn't come from Nikon or from a stranger; it came from someone in her social network who was, coincidentally, employed at the same firm. This woman wasn't targeted at random—she was targeted because of her position in the company, information gleaned from sites like LinkedIn, Facebook, and the corporate website.

Case 3: Human Pen Testing
This test operation targeted 3,000 employees by offering them something fun in email. Within two hours, the testers had to stop the operation because they had over 1,000 employees click on the link in the phishing email, despite the red flags that they had put into the message. From that point on, the company used the experience as a teaching tool from that point on to emphasize the need to be on guard.

Continuing Education – Engaging Your Workforce
Educate the users about the surge in cyber-security attacks on organizations like theirs. What are the trends? What are the security people saying? Agencies must also implement the policies that go along with the education, providing guidelines on what to do when they discover something suspicious. It is helpful to use scenario-based learning and reward systems to recognize employees for reporting suspicious activity or material.

Janet Wilson, Program Manager, C^2 Technologies
As a Program Manager for C^2 Technologies, Ms. Wilson has been instrumental in the development of cyber-security awareness training and communication for Federal Government clients. A PMP since 2005, she received her B.S. from Berry College (Mathematics) and an M.A.T. from Georgia State University (Teaching).

Michael Webber, C^2 Technologies
Michael Webber specializes in cyber security services and training, providing expert guidance to C^2's Veterans Affairs and Department of State clients. Before, becoming a cyber-security trainer, Mr. Webber served as a sworn law enforcement officer with a focus on cybercrime for over twelve years. In addition to assisting government and corporate clients with issues surrounding electronic discovery, digital forensics, and data breach investigations, he has developed and provided cyber training in over 26 countries. Mr. Webber is currently a Senior Vice President of Technology with BitSec Global Forensics, a division of Network Designs, Inc. (NDI), a Service Disabled Veteran Owned Small Business (SDVOSB).

Hiring and Managing a Cyber Security Workforce: What Federal Managers Need to Know
President Obama has declared the "cyber threat is one of the most serious economic and national security challenges we face as a nation" and that "America's economic prosperity in the 21st century will depend on cyber security."

Federal agencies are under pressure to comply with federal cyber mandates and guard against internal and external threats. They will need a workforce capable of doing so. How can agencies make sure they hire and develop the right people in an environment of challenges such as: competition with the private sector for the same skill sets; an evolving field with new and emerging competencies, certifications, and career paths that are still being defined; and a preponderance of tech-savvy younger, "Gen Y" workers with unique motivations and drivers?

A 2009 Partnership for Public Service Report revealed four primary challenges that threaten the quality and quantity of our federal cybersecurity workforce.

1. The pipeline of potential new talent is inadequate.
2. Fragmented governance and uncoordinated leadership hinders the ability to meet federal cybersecurity workforce needs.
3. Complicated processes and rules hamper recruiting and retention efforts.
4. There is a disconnect between front-line hiring managers and government's HR specialists.

Federal managers responsible for workforce planning and development must understand the unique aspects of the cyber security workforce and how to ensure that the right recruitment, training, performance management, and retention programs are in place to meet the grown demand for these skills. They also need to understand when hiring for a skill set is less attractive than contracting for it.

Scott J. Cameron, Senior Vice President, R3 Government Solutions, LLC.

Scott J. Cameron is Senior Vice President at R3 Government Solutions, where he leads the human capital management consulting practice. R3 is a service-disabled Veteran owned small business that provides federal agencies with powerful transformational capabilities in business process, human capital, and information technology to promote mission accomplishment. Scott is a Fellow of the National Academy of Public Administration, and also writes a bi-monthly column on government human capital management issues for HR News, the publication of the International Public Management Association for Human Resources. He is registered as a Certified Professional by the International Public Management Association for Human Resources, and elected as a CHCO SAGE with the Partnership for Public Service.

Before entering consulting, Scott was a Deputy Assistant Secretary at the Department of the Interior. He was Chief Human Capital Officer, E-Government Executive, had the lead on budget and performance integration, and served on the Executive Committee of the interagency Chief Acquisition Officers Council. He was also the Managing Partner of two of OMB's government wide E-Gov projects; Geospatial One Stop and Recreation One Stop.

Before joining Interior, he established the global government relations function for CHEP. CHEP is the global leader in materials handling, with business in 38 countries. Earlier, Scott was Deputy Chief of the Interior Branch at the Office of Management and Budget (OMB), part of the Executive Office of the President. He served as the program examiner for the US Geological Survey, US Fish and Wildlife Service, and the National Biological Survey. Earlier at OMB, he oversaw the EPA's Office of Water and the Office of Research and Development.

Scott began his career as a Presidential Management Intern in the U.S. Fish and Wildlife Service, after earning a BA in biology from Dartmouth College, and an MBA from Cornell University. He was raised in New York City, is married, and has a son.

	TRACK 1: Green Auditorium	
12:15 – 1:10 pm	Lunch Provided – NIST Cafeteria Rear	
1:10 – 1:40 pm	**Presentation of FISSEA Security Contest Winners:** Contest Coordinator: Gretchen Morris, DB Consulting/NASA **Presentation of 2012 FISSEA Educator of the Year, J. Paul Wahnish:** By Susan Hansche, Avaya/Dept.of State, FISSEA Educator of the Year for 2011	
	TRACK 1: Green Auditorium	**TRACK 2: Lecture Room B**
1:45 – 2:30 pm	**Mitigating the Top Five Human Risks** Lance Spitzner, The SANS Institute	**Moving into a Future of Training and Education Centered Around Lifelong Learning** Dr. Rae Hayward, $(ISC)^2$

Mitigating the Top Five Human Risks

Organizations are learning that no matter how much they invest in technology, cyber attackers will continue to compromise the human element. Organizations must start securing the HumanOS, and one of the primary ways to do that is through high-impact security awareness and education. However most organizations are overwhelmed at where to start. Traditionally awareness has been compliance driven, attempting to truly change human behavior is a far harder challenge. This talk will address this challenge in two parts. First, we will discuss a community research project that has identified the top human risks to most organizations, allowing them to prioritize which human risks to focus on. The second part of the talk will focus on how organizations can design a roadmap to build, maintain and measure a high-impact awareness program that addresses those very risks. All materials and resources were developed by the community and are freely available for anyone to use.

Lance Spitzner, The SANS Institute

Mr. Lance Spitzner is an internationally recognized leader in the field of cyber threat research and security training and awareness. He has helped develop and implement numerous multi-cultural security awareness programs around the world for organizations as small as 50 employees and as large as 100,000. He invented and developed the concept of honeynets, is the author of several books, and has published over thirty security whitepapers. Mr. Spitzner started his security career with Sun Microsystems as a senior security architect, helping secure Sun's customers around the world. He is founder of the Honeynet Project; an international, non-profit security research organization that captures, analyzes, and shares information on cyber threats at no cost to the public.

Mr. Spitzner has spoken to and worked with numerous organizations, including the NSA, FIRST, the Pentagon, the FBI Academy, the President's Telecommunications Advisory Committee, MS-ISAC, the

Navy War College, the British CESG, the Department of Justice, and the Monetary Authority of Singapore. He has consulted around the world, working and presenting in over 20 countries on six different continents. His work has been documented in the media through outlets such as CNN, BBC, NPR, and The Wall Street Journal. He serves on the Distinguished Review Board for the Air Force Institute of Technology, Technical Review Board for CCIED, and the Information Assurance Curriculum Advisory Board at DePaul University. Before working in information security, Mr. Spitzner served as an armor officer in the Army's Rapid Deployment Force and earned his MBA from the University of Illinois-Chicago.

Moving into a Future of Training and Education Centered Around Lifelong Learning

Government agencies need to fill their many open information security jobs with qualified personnel. To do this, agencies must hire not only more information security professionals but also somehow retain their existing employees by offering advanced training and education opportunities equal to what is offered by other higher-paying employers.

Traditionally, training and education has been utilized primarily for helping individuals increase industry expertise and knowledge or prepare for certification examination. These training courses have been delivered via traditional methods of instructor-led, live online, and through printed textbooks. However, according to $(ISC)^2$ research, the gap between demand for qualified information security professionals and the low supply has further widened, which makes it imperative for organizations to embrace a new approach to training and education. That approach must be centered around "lifelong learning" that caters to the spanning needs of students, young professionals, and seasoned professionals in the field.

In this session, Dr. Rae Hayward, EdD, Sr. Education Development Manager at $(ISC)^2$, will discuss the benefits of a lifelong learning approach and the challenges that must be overcome.
Attendees to this session will gain understanding of the importance of:

- Evaluating educational content for effectiveness
- Identifying and solving industry needs
- Aligning curriculum at every stage of learning among universities, colleges, industry, certification and professional organizations
- Expanding delivery methods beyond traditional training/education platforms
- Creating and implementing educational programs that increase awareness and provide guidance on compliance and regulations

Dr. Rae Hayward, Senior Manager of Product Development, $(ISC)^2$

Rae is currently the Senior Manager of Product Development for one of the world's largest IT Security Certification Associations. The association specializes in IT Security Certification, and has over 85,000 global members. She is responsible for the strategic development of all educational content, which includes developing courses for the entire career lifecycle of an IT Security professional. Educational content is developed for the onboarding process at the K-12 level, all the way to the industry professional and their continuing education requirements.

In addition Rae has taught college level courses for several years both face-2-face and online, she has experience in corporate training and development. She has a Bachelor in Finance, a Masters in Finance, and a Doctorate in Instructional Technology and Distance Education, and in General Education from Nova Southeastern University. On a more personal note, her dissertation is titled "Increasing Motivation and Transfer of Learning in Online Environments Through Application of Cognitive Load Principles". The research conducted throughout this processes helped her to form her own theory on learning and education. As we go through life, we experience many things, process thoughts on various levels, and interact with an abundance of people who are both different and similar to us. From these experiences we develop new ideas and grow in our tolerances, so being able to recall these experiences and share with others, we continue to increase our knowledge. Applying what we have learned to task-relevant situations whether at work or in our personal lives, increases our ability to retain and utilize this knowledge for future application.

	TRACK 1: Green Auditorium	TRACK 2: Lecture Room B
2:35 – 3:00 pm	**NIST SP 800-16 Update** Patricia Toth, NIST	**FREE Federal Training Resources** Benjamin Scribner, DHS/NPPD/SECIR
3:00 – 3:15 pm	Afternoon Networking Break	

NIST SP 800-16 Update

This presentation will discuss the current efforts to develop NIST Special Publication 800-16 Rev2 (Draft) "Information Security Training Requirements: A Role and Function Based Model".

Since the release of Draft SP 800-16 Rev 1 in 2009 and the original publication of SP 800-16 in 1998 the roles and responsibilities of information security personnel have greatly expanded. The new Draft SP 800-16 will provide a comprehensive training methodology for the development of training modules for roles identified as having significant information security responsibilities.

Patricia Toth, Supervisory Computer Scientist, NIST

Pat is a Supervisory Computer Scientist in the Computer Security Division at NIST. Pat has worked on numerous documents and projects during her 22 years at NIST including the Common Criteria Evaluation Program, served as Program Chair for the National Computer Security Conference, the FISMA family of guidance documents including SP 800-53 and SP 800-53A, the National Initiative for Cybersecurity Education (NICE), and FISSEA.

FREE Federal Training Resources

In 2010, President Obama established the National Initiative for Cybersecurity Education (NICE). The mission of NICE is to enhance the overall cybersecurity posture of the US by accelerating the availability of educational and training resources. The Federal Virtual Training Environment (FedVTE) and the Federal Cybersecurity Training Events (FedCTE) directly addresses the NICE mission by accelerating the availability of training resources for the current and future U.S. cybersecurity workforce.

FedVTE is a flexible, multi-media, e-learning environment that federal employees can access anywhere, anytime. The Department of Homeland Security (DHS) partnered with the Departments of State (DoS) and Defense to establish the FedVTE program. FedVTE is based on a proven and mature Department of Defense (DoD) technology that supplements DoD Service training. FedVTE currently has the capacity to support up to 125,000 military, civilian and contractor personnel. As compared to the DoD legacy system, FedVTE has an easier to use interface and new courses. It also offers organization-specific reports for agency managers and a Content and Configuration Board is dedicated to keeping the training current and relevant.

The FedVTE content library contains pre-recorded classroom training that users can access anytime, anywhere. Audio and video recordings are synchronized with a transcription and instructor slides. If users pause or exit, FedVTE will remember where they left off. Additional features include:

- 550 hours of training, 150 demos, and 3,000+ pieces of content
- Fast forward, rewind, highlight text, and add personalized notes
- View and print training certificates and progress reports

Many FedVTE courses also include hands-on labs. Users practice the learning concepts on computers in a sandbox network. When the lab is complete, FedVTE restores settings and provisions the sandbox to another user. Labs are currently included in 60 FedVTE courses.

The FedCTE program provides learning and networking opportunities as well as hands-on experience. Courses are scheduled throughout the year. Features include:

- 1-3 day courses scheduled throughout the year on a wide range of cybersecurity topics
- Students are handpicked to facilitate networking and cross-governmental sharing of best practices
- Activities that allow students to apply the learning concepts in a hands-on environment
- Courses delivered in both traditional and virtual classrooms

Mr. Benjamin Scribner, DHS/NPPD/SECIR

Benjamin Scribner has eight years of experience developing cybersecurity and workforce improvement policy and initiatives for the Departments of Defense (DoD) and Homeland Security (DHS). He leads a coalition of US federal training organizations to develop government-wide resources for cybersecurity professionals. Mr. Scribner is responsible for the Federal Virtual Training Environment and Cybersecurity Training Events program.

	TRACK 1: Green Auditorium	TRACK 2: Lecture Room B
3:15 – 4:00 pm	**Entry-Level CyberSecurity Analyst Skill Development** Brian Ford and James Risler, Cisco Systems	**Continual Evolution and Maturation: Garnering Executive Support, Creating a Brand, Educating Employees** Gared Chastain and Jayme Jordan, Raytheon Co.

Entry-Level Cyber Security Analyst Skill Development

Understand the process of how a security analyst develops their skills and how an organization can facilitate this process. This session discusses the job role of a security analyst and the complex nature of learning how to identify threats and intrusions on the network with the variety of technology products and SIEM (Security Information and Event Management) tools available. The responsibilities often include the following areas: monitoring, traffic analysis, event and alarm handling, and incident response. Analysts are often asked to be knowledgeable of specific tools and be able to implement these tools to gather data across networks. This presentation will outline how Cisco has identified and worked with subject matter experts in intrusion analysis and operations; then incorporated their subject and process expertise into a course which seeks to develop the knowledge in the entry-level security analyst.

We will discuss the challenges that Cisco faced building a lab that would help an entry-level security analyst obtain the skills necessary to start analyzing traffic and identifying known and unknown threats. The presentation will outline how our lab environment uses known threats such as Denial of Service (DoS) network attacks to train the students and develop their skills.

Other topics included in this discussion include why are PCAP files important and what can Netflow show a security analyst? What historical threat signatures and packet payloads can be used to develop an individual's capabilities? Finally, what can one learn from this process for training individuals to take over highly technical roles within an information security group?

Brian Ford, Consulting Engineer and James Risler, Security Education Specialist Cisco Systems

Brian Ford is a Consulting Engineer in the Corporate Consulting Group, part of the Office of the Chief Technology Officer of Cisco Systems the worldwide leader of networking for the Internet. Brian has actively participated in the development of Cisco security products including the security appliance and access control solutions. His current research areas are Cybersecurity, access control, and security analytics. He consults regularly with staff and executives from companies in a variety of fields to help create synergistic solutions to network and Internet security problems. In his 15 years at Cisco, Ford has supported customers ranging from small Internet-based charitable organizations and educational institutions through large multinational corporations and international governments. Born and raised in New York; Brian lives with his wife and son on the north shore of Long Island. Ford was formerly a CCIE (#2106) and is a current Computer Information Systems Security Professional (CISSP) and active supporter of technical education through the Cisco Networking Academy program. He received a B.S. in Computer Science from the State University of New York at Stony Brook and is currently pursuing a Masters in Information Assurance from Norwich University.

James Risler, CCIE No. 15412, is a systems engineer and technical education consultant for Cisco Systems. His focus is on security technology and training development. James has more than 20 years of experience in IP internetworking, including the design and implementation of security solutions for enterprise networks. Mr. Risler is responsible for helping to design and develop the variety of security training courses that Learning@Cisco produces.

Prior to joining Cisco Systems, James provided Cisco security training as a Cisco CCSI and consulting for Fortune 500 companies and government agencies. He has two bachelor's degrees from University of South Florida and a MBA in Information Technology from The University of Tampa.

Continual Evolution and Maturation: Garnering Executive Support, Creating a Brand, Educating Employees

Raytheon is a technology and innovation leader specializing in defense, homeland security and other government markets throughout the world. With a history of innovation spanning 90 years, Raytheon provides state-of-the-art electronics, mission systems integration and other capabilities in the areas of sensing; effects; and command, control, communications and intelligence systems, as well as a broad range of mission support services. Raytheon maintains offices in 19 countries and has established global companies to serve customers in the United Kingdom, Australia, Spain, France, Germany and Canada.

Raytheon Company employs over 70,000 employees, making it challenging to ensure that all of our employees are aware of the cybersecurity threats our company faces and the risks they face at home. To that end, in 2007 RTN Secure was created. The RTN Secure program's goal is to educate employees about the growing problem of cyber crime, its potential effects on our company and how changes in the way we protect the company will affect Raytheon employees. RTN Secure is an awareness campaign that provides tips, tools, updates and other information on how employees can play their part in Raytheon's information assurance efforts.

This presentation will discuss Raytheon's RTN Secure program. We will focus on how we developed the brand, obtained executive support and now apply the brand for high-visibility initiatives and communications. The discussion will touch upon the challenges involved in developing a consistent and recognizable brand, the lessons learned and the evolution of the program over the last 5 years.

Gared Chastain, Information Assurance Manager; Jayme Jordan, Enterprise IT Security Learning, Raytheon Company

Gared Chastain is the manager of the Vulnerability Management organization at Raytheon located in Garland, TX. His team is focused on the management of vulnerabilities consistent with risk tolerance levels and the development of education within the system development lifecycle.

In his prior role beginning in 2009, he served as the program manager for the RTN Secure program, an internal risk management program focusing on the mitigation of information security threats through technology deployment and user education, located in Garland, TX.

In 2008, he served as the Executive Support Lead to the executive staff of IIS. He was responsible for the executive IT support operating model and service delivery. In this role, he ensured consistent service quality and delivery to the executive staff at all IIS business sites. In parallel, Gared aided in the business evaluation of the IT Integrated Sourcing Initiative (IT ISI) coordinating logistics and communications necessary to the greater IIS IT Evaluation Team for the Raytheon IT Supplier

agreement.

Prior to his position in IIS, Gared served as the Global Enterprise Architecture (GEA) Operations Manager in Corporate IT, where he was responsible for the daily operations of the GEA. His primary focuses were to the deployment of an enterprise architecture platform which provides improved visibility into the Raytheon architecture through enabling multiple system integration across the enterprise and to convey the enterprise architecture touch points within the IPDS process.

Gared holds a bachelor of science in Computer Engineering with a minor in Mathematics and Business and a master of science in Management of Information Systems both from Texas A&M University. He also completed his CNSS/ISSO Management of Information Assurance & Security Certificate while at Texas A&M University. Chastain also has certifications as a Raytheon Six Sigma Specialist and ITIL v3 Foundation.

Jayme Jordan is the enterprise leader for RTN Secure, an internal risk management program focusing on the mitigation of information security threats and user education. Located in Garland, Texas, Jayme has held this position since October 2007. Jayme is responsible for developing and deploying an IT Security Learning Program encompassing awareness and training level learning artifacts for roughly 72,000 global employees as well as training and education level learning for IT and IT Security Professionals throughout the company. She leads an enterprise network of IT Security Learning Leaders to deploy metrics-based learning artifacts and initiatives. In her role, Jayme also consults with Fortune 500 business partners on Information Assurance learning best practices and methodologies.

Jayme holds a Bachelor of Science degree in Computer Science from the Erik Jonsson School of Engineering and Computer Science at the University of Texas at Dallas. She also holds Certified Information Systems Security Professional (CISSP), Certified Information Systems Auditor (CISA) and Certified in Risk and Information Systems Controls (CRISC) professional certifications. She is an active member of the Federal Information Systems Security Educators' Association (FISSEA) and The Colloquium for Information Systems Security Education (CISSE). Jayme completed her certification as a Raytheon Six Sigma Specialist in 2008.

	TRACK 1: Green Auditorium	
4:05 – 4:40 pm	**Bridging the Gap Between Education, Professionalism, and Professional Certifications Panel** G. Mark Hardy, National Security Corp., Moderator; David Kim, Security Evolutions, Inc.; Michael Goldner, ITT Technical Institute; Wen Liu, ITT Educational Services, Inc.; Christopher Will, Jones and Bartlett Learning	

Bridging the Gap Between Education, Professionalism, and Professional Certifications

Academic programs often emphasize theoretical learning, while professional certifications emphasize hands-on skills or practical knowledge. This panel will address the gap between education, professionalism, and professional certifications, and how all of these objectives can be accomplished concurrently with foresight, careful curriculum development, and a skilled instructor base.

The requirement to educate and field a cyber security workforce is not new. In February 1993, the foreword of National Security Telecommunications and Information Systems Security Committee (NSTISSC) No. 500, "Information Systems Security (INFOSEC) Education, Training, and Awareness," now known as the Committee on National Security Systems (CNSS), stated:
"Education, training, and awareness are countermeasures that effectively reduce exposure to a variety of known risks. In order to achieve this end, it is essential to have a federal work force that is aware of, and educated about, the problems of information systems security (INFOSEC)."*

Yet nearly twenty years later, we still find a significant gap between the requirements of an educated federal work force and the number of graduates of cyber security educational programs. Yet there are successes that can be modeled, and serve as templates for academic institutions to rapidly field certified cyber security educational programs.

The panel will discuss the efforts involved to build a certification-granting degree program. Jones & Bartlett Learning's original blueprint for the Information Systems Security & Assurance (ISSA) curriculum was based on imbedding key learning objectives from the industry's leading professional certification in information systems security and information assurance. With this goal in mind, the object is not to teach the professional certifications, but to prepare the students with content and learning outcomes that align to these professional certifications. Currently, the ISSA curriculum maps to the following industry leading professional certifications:

- CompTIA's Security+
- $(ISC)^2$ Systems Security Certified Professional (SSCP®)
- $(ISC)^2$ Certified Information Systems Security Professional (CISSP®)
- NSA 4011 Standard for Information Systems Security Professionals
- NSA 4013-Advance Standard for System Administrators Performing Information Assurance

The content and curriculum developers ensured that students would be better positioned to rapidly assume workforce recognition by achieving a degree that maps to key information systems security and information assurance standards and professional certifications. One of the key differentiators developed by Security Evolutions, Inc. for Jones & Bartlett Learning was the creation of 130, hands-on skills-set readiness labs. This "hands-on" approach to providing students with the skills-sets and competency for performing information systems security assessment and audits helps bridge the gap between education, professionalism, and professional certifications. This panel presentation provides a unique perspective of multiple stakeholders, including Publisher, Security Consultant & Hands-on Lab Developer, Educator, Professor/Instructor, Student, and the Employer/Hiring Company, which represents a complete ecosystem for cyber security education, professionalism, hands-on skills-set readiness, and professional certification.

After approximately 30 minutes of questions and answers prepared for the panel, this session will open to audience questions so that attendees can gain in more detail an understanding of this process. * - http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA362604

Panel members: G. Mark Hardy, President, National Security Corporation (Moderator); David Kim, B.S.E.E., President & Chief Security Officer for Security Evolutions, Inc. (SEI); Michael Goldner, ITT Technical Institute; Wen Liu – National Chair, School of IT, ITT Educational Services; Christopher Will, Jones and Bartlett Learning

G. Mark Hardy has over twenty-five years experience in information systems with emphasis on cyber security. Extensive experience as security consultant to multiple industries. Wrote, produced, and presented over 200 security seminars nationwide. Popular keynote at major security conferences. Significant work in cyber security and electronic commerce. Progressively increasing responsibility for project management, application design, and developing technical solutions to business requirements.

Mr. Hardy developed a national organization for military leadership training; hired, trained, equipped, and fielded 180 facilitators, established 72 training sites across the nation, created and validated curriculum, and achieved throughput of over 10,000 students. In addition, Mr. Hardy acted as the senior subject matter expert providing technical Quality Assurance Review for the Jones & Bartlett Learning Information Systems Security & Assurance (www.issaseries.com) curriculum.

David Kim, B.S.E.E., is the President & Chief Security Officer for Security Evolutions, Inc. (SEI) located outside of the Philadelphia metropolitan area. SEI provides IT security training and consulting services for US-based international airports, large enterprises, banking, financial, manufacturing, healthcare, and retail verticals around the world. SEI has specific expertise and experience in enterprise IP data networking infrastructures, and VoIP and SIP layered security solutions where privacy data may encompass both data and voice communications.

In 2008, Mr. Kim was hired by Jones & Bartlett Learning Publishers as the lead IT Security & Information Assurance curriculum architect for their Information Systems Security & Assurance (ISSA) program (www.issaseries.com). The ISSA curriculum recently was awarded the coveted NSA 4011 and NSA 4013-Advanced certification designation for mapping the curriculum's core learning objectives to both of these standards. The ISSA curriculum is completely digital, allowing for customized and blended content delivery. The ISSA curriculum consists of 13 textbooks, 13 on-ground and on-line courses, and 130 skills-set readiness hands-on labs. These 130 skills-set readiness labs were developed by SEI including the technical and security requirements for the Virtual Security Cloud Lab (VSCL) environment. These labs provide students with the necessary hands-on experience to perform information system security and information assurance activities on today's IT infrastructures.

Previously, Mr. Kim was the Chief Operating Officer (COO) of (ISC)2 Institute located outside the metropolitan Washington, D.C. area in Vienna, VA where he was responsible for content development, educational product development and management, and educational delivery and fulfillment for (ISC)2 (www.isc2.org) and their flagship professional certifications CISSP® and SSCP®. Mr. Kim was also involved in the initial launch of the CISSP® Concentrations: ISSAP®, ISSMP®, ISSEP® to provide more granular professional certifications in security architecture, management, and engineering.

Michael Goldner is the Dean of Academic Affairs for ITT Technical Institute in Norfolk Virginia, where he teaches bachelor level courses in computer network and information security systems. He also serves on the ITT Educational Services Inc. National Curriculum Committee on Information Technology. He received his Juris Doctorate from Stetson University College of Law, his undergraduate degree from Miami University and has over fifteen years working in the area of Information Technology. He is an active member of the American Bar Association, and the Cyber Law committee. He is a member of IEEE, ACM and ISSA, and serves as the

Educational Officer for the ISSA Hampton Roads Chapter. He holds a number of industrially recognized certifications including, CISSP, CISM, CEH, CHFI, CEI, MCT, MCSE/Security, Security +, Network + and A+.
Michael completed the design and creation of a computer forensic program for ITT Technical Institute, and has worked closely with Jones & Bartlett Learning in the creation of their Information Systems Security & Assurance series.

Wen Liu is the National Chair of the School of Information Technology at ITT Educational Services, Inc. (ITT/ESI), which operates 140+ ITT Technical Institutes in over 35 states. During his tenure with ITT/ESI, Mr. Liu created a dozen or so associate's and bachelor's programs in information technology, including the bachelor's program in Information Systems Security (ISS) and Information Systems and Cybersecurity (ISC) offered in the entire ITT Technical Institute system nationwide. Mr. Liu holds a Master of Science degree in Information and Communications Sciences and a Master of Arts degree from Ball State University in Muncie, Indiana. Prior to joining ITT/ESI, Mr. Liu was a telecommunications analyst at the state government of Indiana. Mr. Liu is an active member of IEEE Computer Society and IEEE Communications Society. In addition, Mr. Liu serves on the advisory board for the Microsoft Official Academic Courses (MOAC) with John Wiley & Sons. Mr. Liu played an instrumental role in the education and industry partnership initiative between ITT/ESI and Jones & Bartlett Learning in the design, creation and implementation of the curriculum resources for the information systems security program offered at ITT Technical Institute.

Christopher Will is the Senior Vice President of Digital Curriculum Solutions at Jones and Bartlett Learning. He is the Publisher of the Information Systems Security & Assurance Series (www.isssaseries.com), the first publisher book and curriculum series to meet the rigorous National Security Agency's 4011 Standard and 4013-Advanced National Training Standards for Information Systems Security and Information Assurance. A graduate of the University of Virginia, Mr. Will has 25 years of experience in the publishing and e-learning industry in the academic, government, trade, and professional space.

	TRACK 1: Green Auditorium	
4:45 pm	Prize Drawing	
5:00 pm	Dinner Get Together – Location TBD (Sign up at conference. Dinner is not included in the registration fee. Each person will pay for self.)	

Wednesday, March 20, 2013 – Vendor Exhibit Day

8:00 – 8:45 am	Registration, Breakfast, and Networking
8:45 – 9:00 am	Morning Announcements Daily Announcers: Track 1: Louis Numkin Track 2: Cheryl Seaman
9:00 – 9:40 am	**Keynote Address: Green Auditorium** Mr. Bryant G. Tow, *CISSP,C-CISO, CHS III,* Vice President, InfraGard National Members Alliance Chief Security Officer, Independent

Keynote Address:

PIAA companies have begun to embrace new channels and technologies that increase the efficiency of their operations, such as social media, cloud computing, and mobility. These tools offer new opportunities, but also raise serious concerns about the security of the protected information of your company, your customers, and your staff. How good a job are you doing in defending against the threats posed by a new generation of cyber-criminals? Fortunately, there are information security programs available to ensure compliance, protection of applications, and disaster recovery. This session will focus on cyber-security risks and what steps can be taken to protect intellectual property. Mr. Tow will review essential resources for ongoing operations and offer insights on how top businesses keep pace with cyber-security challenges.

Bryant G. Tow, CISSP,C-CISO, CHS III, Vice President, InfraGard National Members Alliance , Chief Security Officer, Independent

Bryant has over 20 years of experience in the IT industry both as an entrepreneur and senior executive. Bryant has held responsibilities within all aspects of the security industry including: thought leadership in the area of cyber security, award winning development of security solutions, go-to-market and business development strategies, managing large global cyber and physical security teams. Bryant currently works as a thought leader in the security industry and a trusted advisor by regularly meeting with clients, speaking at industry events, working with industry analyst, media outlets and law enforcement. As the recent Chief Security Officer for CSC's Financial Services Group (FSG), Bryant enhanced the security posture of the FSG solutions and quantifiably reduced risk by developing the global security strategy and executing necessary programs to ensure the confidentiality, integrity and availability of FSG's intellectual property. Bryant has held several leadership positions in the security industry including the Department of Homeland Security and the FBI and is currently serving as a Vice President of the InfraGard National Members Alliance an FBI public/private alliance program boasting over forty-five thousand members and is recognized as a Ponemon Fellow by the Ponemon Institute, the industry's leading industry research organization. Bryant has published several books and articles on cyber security topics and has received several awards including "Governor's Office of Homeland Security Award for Exceptional Contribution in Recognition of Outstanding Support of Tennessee's Counter Terrorism Program.

	TRACK 1: Green Auditorium	
9:40 – 10:10 am	**Workforce Development through Cybersecurity & Project Management Training and Certifications** Dr. Jo-Ann Rolle, Consultant, Moderator; Leo Dregier III, The Security Matrix; Jerry Perone, National Management Center	

Workforce Development through Cybersecurity & Project Management Training and Certifications

The panel discussion will overview the current demand and supply for cybersecurity and project management professionals. The panelists will give insights on cybersecurity and project management training; lessons learned; and tips for successful preparation for certifications.

Additional topics will include:

- How the certification landscapes have changed in the past and where are they going in the future.
- The impact of DoD 8570
- The old project management approach and the practical application in today's world.

Dr. Jo-Ann Rolle, Consultant; Leo A. DregierIII, CEO, PMP, and Trainer Principal, The Security Matrix, LLC; Jerry Perone, CEO, PMP, ACP, and Trainer President, National Management Center

Dr. Jo-Ann Rolle has extensive executive management experience in higher education, corporate and government operations including, marketing, forecasting, economics, information technology, data projection and budget oversight.

Throughout her career, she has been involved in defining strategic deliverables, re-shaping integrated program implementation, generating cohesive work processes, and is recognized for leading change and streamlining functions in small and large organizations.

Dr. Rolle earned her Bachelors of Business Administration from the University of Miami, a Master's Degree from Southern Illinois University in Economics, and a Ph.D. in Economics from Howard University. She has received numerous awards and nationally recognized achievements of Excellence in Leadership and Management.

Jerry Perone Mr. Perone is a seasoned executive, an entrepreneur, author, speaker and consultant. He has been responsible for all aspects of business and project-program management (P/PM); has been on the Board of seven companies, as well as starting and operating several of his own businesses. He is the author of the book "Entrepreneur Boot Camp" and the host of WBZS Business Radio's Weekly Show by the same name.

At IBM, Mr. Perone rose to the rank of the Global Portfolio Management Executive, reporting to the IBM World Wide General Manager - Global Services for the Financial Services Sector. In this capacity he oversaw a portfolio that had grown to a total contract value of over $10B. During his tenure at IBM, he implemented dashboards, program management, risk management, knowledge management, business controls and auditing standards and procedures resulting in the portfolio being rated "#1 in the World" by independent auditors evaluating IBM. He also designed and developed a trouble project assessment and recovery SWAT Team who in 2000 performed a worldwide troubled project assessment with successful recovery for the 2000 Sydney Olympics. He has been an adjunct professor of Project Management for several universities. Mr. Perone earned his BS in Electronic Technology from the University of Dayton, and a MBA in Finance & Accounting. Mr. Perone can be reached at jerry.perone@verizon.net.

Leo A. Dregier III Leo has been a principal at the computer security firm The Security Matrix, LLC since 1995. Leo has held over 40+ career certifications relating to computer networking, information assurance, forensics, project management, and cyber security. He has provided consulting services to many federal clients to include The Department of State, The Department of Labor, The Internal Revenue Service and The Centers for Medicaid and Medicare. Additionally, he has helped thousands of IT professionals achieve their certifications online at TheCodeOfLearning.com and maintains an evaluation level above 90+%. When Leo is not working as a consultant or in the classroom, you can find him working on his other personal projects. TheProfitCycle.com is geared towards people who need help learning how to adapt to technology and want to make money using technology as a solution. Leo has also created FindRealEstateHelp.com, which is a real estate problem solving and investment company. In his spare time spends time with his beautiful wife. You can contact him at LeoDregier.com

10:10 – 10:40 am	**Vendor Exhibit Hall Open – Flag Hallway – Open 10:00 – 3:00 pm** **First opportunity to visit**	
	TRACK 1: Green Auditorium	**TRACK 2: Lecture Room B**
10:40 – 11:30 am	**The Unintentional Oversharing of Information** Dr. Karen Paullet, American Public University	**Professionalizing the Nation's Cybersecurity Workforce** Edward Nyack, Department of Homeland Security

The Unintentional Oversharing of Information

Sharing information online or via social network sites could potentially expose users to becoming victims of a cyber-related crime. As more people begin to use social networking sites they are becoming more vulnerable to cyber-criminals. As people post personal data the distribution of this information might not be in their control. Cyber-criminals can easily search for a victim without ever leaving their house. Many users of social network sites are not aware of the possible pitfalls of failing to secure their personally identifiable information by using the privacy settings of the site. A failure to properly secure their profile information can lead to disaster. It is imperative that people understand the possible implications of the information that can be obtained from their profiles. Raising awareness of privacy control mechanisms, privacy best practices, and possible consequences of unprotected information-sharing is necessary to protect our personal information.

Dr. Karen Paullet, American Public University

Dr. Karen Paullet has been a faculty member at American Public University System since May of 2009 where she teaches Cyber Security. She holds a BS in Information Systems, a MS in Communications and Information Systems, and a DSc. in Information Systems and Communications from Robert Morris University. In addition Dr. Paullet has spent over 13 years working with law enforcement preparing cases using digital evidence for trial. She has spoken at over 100 engagements throughout Pennsylvania on the Dangers of Social Network Sites, Cyberbullying, Cyberstalking and the CSI Effect. She has applied her research interests to educate students, organizations and law enforcement throughout Pennsylvania. Her work has been published through various outlets to include the International Association for Computer Information Systems (IACIS), the Information Systems Educators Conference (ISECON), the Conference on Information Systems Applied Research (CONISAR) and The Institute for Operations Research and Management Sciences (SEInforms). She brings her professional experience in law enforcement and teaching to serve and educate others in the community.

Professionalizing the Nation's Cybersecurity Workforce

The National Initiative for Cybersecurity Education (NICE) has been chartered to characterize the current cybersecurity workforce development landscape, and propose criteria that federal, state, local, and tribal organizations can use to identify which careers within the cybersecurity field may require professionalization. To evaluate different approaches and tools for professionalization, the government commissioned the National Academy of Science (NAS) to examine this question through a series of national forums. Held from December 2013 through March 2013, the workshops are open to participation by all cyber professionals across Federal, State, Local, and tribal governments, industry and academia. The workshops will address topics such as the expected level of preparation, proficiency, and competence of cybersecurity professionalization, to include certification and licensing. This workshop session will provide an update on both the initial findings from the forums and progress of the study by NAS. The committee's final report will be released in the summer of 2013.

Edward Nyack, National Cybersecurity Education Office (CEO), DHS

Replacement speaker for Robin "Montana" Williams, DHS

	TRACK 1: Green Auditorium	TRACK 2: Lecture Room B
11:35am – 12:05pm	**Securing Your Agency's Future with CyberCorps®: Scholarship for Service** Kathy Roberson, Cyber Corps®: Scholarship For Service (SFS) Program	**Ten Commandments of Effective Security Awareness Training** Ralph Massaro, Wombat Security Technologies, Inc.

Securing Your Agency's Future with CyberCorps®: Scholarship for Service

The Cyber Corps®: Scholarship for Service (SFS) program is a component of the Federal Cyber Service (FCS) Training and Education Initiatives. The SFS program is co-sponsored by the National Science Foundation and the U.S. Department of Homeland Security. This initiative reflects the critical need for Information Technology professionals specializing in information assurance and security. The SFS Program trains high-caliber students from institutions designated by the National Security Agency (NSA) and DHS as Centers of Academic Excellence in Information Assurance Education (CAE/IAE).

Through this program NSF provides scholarships to students in cyber-security in exchange for Federal service upon graduation. The program began in 2000 to help Federal agencies meet their Information Assurance needs and strengthen their cyber space lines of defense. Through this program, we have built a candidate pool of superbly qualified IA graduates from over 40 Centers of Academic Excellence in Information Assurance Education. Because these students receive NSF-funded scholarships and stipends in exchange for service upon graduation, they must make themselves available for Government employment anywhere in the continental United States. Since 2000, SFS scholarships have been awarded to more the 1,500 students.

Finding the talent needed to protect the information systems at Federal agencies can be challenging. The SFS program helps hiring managers at Federal agencies by selecting the finest candidates to participate through a competitive process at NSF-selected, CAE/IAE designated institutions. Students become part of a select pool of candidates you may recruit for internships during their academic term and permanent placement after graduation.

While the SFS program covers the costs of study, the employing agency is responsible for the student's salary and applicable benefits during the internship and employment periods, as well as any costs associated with acquiring the required level of security clearance.

Kathy Roberson, Cyber Corps®: Scholarship For Service (SFS) Program

Kathy Roberson is a Human Resources Consultant with the US Office of Personnel Management, Human Resources Solutions. Ms. Roberson has been with OPM since 1987 and is currently responsible for managing the overall administration of the CyberCorps®: Scholarship For Service (SFS) Program. The SFS Program awards scholarships to students pursuing a degree in cybersecurity. In return for the scholarship, students agree to work for the Government in a cybersecurity position. Ms. Roberson tracks the progress of students while they are in the program, coordinates placements, provides tools and advice to students on searching for jobs with the Government, provides advice to agencies on recruiting/hiring SFS students, conducts agency briefings about the SFS program, and participates in the development of policy for the program.

Ten Commandments of Effective Security Awareness Training

While some argue that employees are incapable of taking an active role in cyber security, there is strong evidence that supports the effectiveness of education. Research shows that organizations with well-understood security policies suffer fewer breaches and companies with an ongoing security awareness program are 50% less likely to suffer breaches.

Security officers in organizations around the world have enormous pressure and many responsibilities to protect their organizations from cyber threats. One of the responsibilities, that most security officers will admit they are ill-suited for, is educating users about identifying and avoiding cyber threats. Security officers that retire their old PowerPoint training presentation in favor of new interactive cyber security assessment and awareness training software are seeing positive results—including up to a 70% reduction in susceptibility to employee-targeted attacks, which translates to fewer breaches and lower remediation costs.

Security awareness training is an education problem generally being handled by IT security professionals who have never been trained to educate people. In this session, attendees better understand why it is challenging to provide effective security training. They will be advised to put away their boring lectures and lengthy slide presentations and instead leverage these ten tips that actually help people learn. These ten tips are really Learning Science principles that are the result of decades of research. Using learning science principles can provide immediate, tangible, long-term results in educating employees and improving your company's overall security posture.

Ralph Massaro, Vice President of Sales & Operations, Wombat Security Technologies

As VP of Sales and Operations, Ralph leads Wombat's sales activities while also playing a key role in strategic product planning and marketing activities. Ralph brings extensive sales, marketing and operations experience to Wombat. This includes serving as VP of Sales and Marketing for both Solvaire Technologies and TekMethods and as General Manager of Content Products at LogicLibrary. Ralph was also VP of Worldwide Sales at Janus Technologies. Following the acquisition of Janus by Intraware, he served as VP of ITAM Sales, responsible for all ITAM-related revenue. Earlier, Ralph spent eight years at PassGo Technologies, where he was North American General Manager and VP of Worldwide Sales. While at PassGo, he quadrupled North American revenue and helped to position the company for acquisition by Axent Technologies (Symantec). Ralph began his technology sales career at Duquesne Systems/Legent, where he held several sales and sales management positions. He holds a bachelor's degree in Business Administration from Robert Morris College.

	TRACK 1: Green Auditorium	
12:05 – 1:30 pm	**Lunch Provided in NIST Cafeteria Rear** **Visit the Vendor Exhibits – Flag Hallway**	
1:30 – 2:20 pm	**Measuring Behavior – The 12 Key Metrics for Security Awareness** Michael Murray and Katrina Rodzon, MAD Security, LLC	

Measuring Behavior – The 12 Key Metrics for Security Awareness

Much has been made in recent years about the importance of measurement for security awareness programs. However, the majority of discussion about metrics revolves around three different types of measurement: measuring user compliance, measuring user satisfaction and measuring responses to phishing tests.

This session will go farther and deliver the 12 key metrics of a mature security awareness program and break down how those measurements can be gathered in any environment to create an actual behavioral scorecard or dashboard that leads to a mature program that actually delivers ROI from a security perspective.

This talk will aim to leave attendees with a deep understanding of two key concepts and how to implement them:

1. The measurement gap between most security awareness programs and those that are effective in modifying user behavior
2. The ways that we can easily create metrics from data that our organization has in order to make our programs more effective

The 12 areas of measurement are as follows (detailed metrics and how to gather them will be broken out during the talk):

1. Response and Reporting
2. Sensitive Data Handling
3. Online / Browsing Hygiene
4. Email Hygiene
5. Phishing Resilience
6. Passwords
7. Workplace Situational Awareness
8. Remote Working
9. Device Protection
10. Online Information Hygiene
11. Social Media Sites
12. Physical Security

A measurement program around each of these areas will provide a formal dashboard of performance that can lead to a mature and effective security awareness program.

Mike Murray, Managing Partner, and Katrina Rodzon, MAD Security, LLC

Mike Murray has spent more than a decade helping companies large and small to protect their information by understanding their vulnerability posture from the perspective of an attacker. From his work in the late 90's as a penetration tester and vulnerability researcher to leadership positions at nCircle, Neohapsis, and Liberty Mutual Insurance Group, his focus has always been on using vulnerability assessment through penetration testing and social engineering to proactively defend organizations. As well as being in charge of advanced curriculum here at The Hacker Academy, Mike is also a Managing Partner of MAD Security, LLC, where he leads engagements to help corporate and government customers understand and protect their security organization.

Katrina Rodzon is a behavioral scientist for MAD Security. Her last 9 years have been spent studying psychology and ways to modify and study human behavior. From learning about the power of social pressure on group behavior to how subtle changes in reinforcement can drastically change individual behavior, Katrina has spent the better part of a decade learning how humans

work and now applies that to security awareness. When she is not testing the effectiveness of different methods of training, she helps with everything from curriculum development to security awareness video creation.

	TRACK 1: Green Auditorium	TRACK 2: Lecture Room B
2:20 – 2:40 pm	**PM Break hallway near Green Auditorium –** **Afternoon Vendor Exhibit Hall closes after break (Flag Hallway)**	
2:40 – 3:05 pm	**The Wolf in Sheep's Clothing: Sharing the Knowledge of Supply Chain Risk** Susan Farrand, US Department of Energy	**Awareness Panel** Patricia Toth, Moderator; Carolyn Schmidt, NIST; Joe Garrity, LOC

The Wolf in Sheep's Clothing: Sharing the Knowledge of Supply Chain Risk

The Federal Government relies heavily on commercial information and communications technology (ICT) components and services to support mission-critical networks and systems. With the increasing complexity of this technology and the globalization of the supply chain, the trustworthiness of items in the commercial ICT supply chain has become uncertain. Agencies across the Federal Government are beginning to address the reality of the threat in the global marketplace and the increased opportunities for malicious exploitation of components in critical Federal systems. Practices to mitigate ICT supply chain risk throughout component lifecycles are still evolving and present a training and awareness challenge that goes beyond what is considered traditional cybersecurity capabilities.

The workforce is the most critical link in the protection of Federal information assets, and training and awareness are essential countermeasures that can significantly reduce exposure to data loss and compromise. All employees must develop knowledge and skills in supply chain risk management that are appropriate to their positions. Employees from loading dock workers to procurement specialists to information technology and cybersecurity professionals must understand their responsibilities, as well as the nature of the supply chain threat.

This presentation will address the Federal interest in SCRM activities and discuss the risks to information and information systems injected by supply chain exploitation. Current practices and status will also be addressed, and the challenges of training and raising awareness of all employees in the component lifecycle will be discussed.

Susan Farrand, SCRM Program Manager, US Department of Energy

Susan Farrand, CGEIT, is the Federal Lead for the Enterprise Supply Chain Risk Management (eSCRM) Program in the Office of the Associate CIO for Cyber Security, U.S. Department of Energy. In this position, she also leads the eSCRM Resource Center, which includes SCRM training and awareness, policy, threat analysis, and metrics. She was the Director of Policy, Guidance, and Planning within the cybersecurity office and also worked on strategic initiatives in program management and integrated Smart Grid digital technologies. Sue has more than 29 years experience with the Department in both Federal and contractor positions, specializing in cybersecurity, training and awareness, information architecture, and policy development. Ms. Farrand was a corporate trainer for Allstate Insurance Company, a curriculum developer for Sargent-Welch Scientific Company, and a classroom teacher. She holds Bachelor of Arts degrees in English and Mathematics and a Master of Arts in Organizational Management and is a Partnership for Public Service Senior Fellow.

Security Awareness Programs

Awareness is an important aspect of Federal IT Security Training. While emphasis is often placed on simply meeting the annual security awareness training requirement, it is vital for Federal Agencies to expand their programs beyond meeting the requirements. This panel will discuss new and innovative approaches to security awareness training that will engage users and give them a sense of involvement in security. Developing programs under budget constraints, leveraging security awareness resources and gaining buy-in from management will be discussed.

Patricia Toth, NIST, Moderator; Joe Garrity, Library of Congress; Carolyn M. Schmidt, Senior Program Manager, Information Technology (IT) Security Awareness, Training, & Education, Office of Information Systems Management, U.S. Department of Commerce

See Pat Toth's bio -Tuesday, March 19th NIST SP 800-16

Joe Garrity is the IT Security Awareness trainer for the Library of Congress. In addition to all aspects of awareness training programs and special events, he also handles the Library's IT Security website, and works as a Security Advisor on the Library's C+A program. Mr. Garrity started his IT Security background working on the security program as an ISSO and ITSPM for USDA. His responsibilities also included handling the C+A program for the Grain Inspection/Packers and Stockyards Administration (GIPSA).

An industry veteran for over 15 years, Mr. Garrity has covered all aspects of IT. Beginning as a contractor, he has worked for many areas of the government, including the US Forest Service, the SEC, the US Army Corps of Engineers, and the Department of Justice.

Carolyn Schmidt is a Computer Scientist and senior NIST Program Manager for Information Technology (IT) Security Awareness, Training, and Education. She is responsible for establishing and implementing information system security awareness and training for all NIST staff. In addition, she is responsible for the development and vetting of information security and privacy policy for NIST operations. Her work involves most aspects of security risk management, and requires knowledge of service management practices to bring policies into implementation. Ms. Schmidt's experience has encompassed digital library research, systems administration, web development and design, and development of Department-wide IT security policy. She has spoken at several conferences in support of her work in research and in information system security, was awarded the U.S. Department of Commerce Bronze Medal in this subject area, and is an alumnus of University of Maryland University College and the Commerce Science & Technology Fellowship Program.

	TRACK 1: Green Auditorium	TRACK 2: Lecture Room B
3:10 – 3:40 pm	**Enhancing NASA Cyber Security Awareness from the C-Suite to the End-User** Valarie Burks, National Aeronautics and Space Administration (NASA)	**Cyber Security Awareness Training in the Age of Mobile Devices** David Willson, Esq., Global Knowledge

Enhancing NASA Cyber Security Awareness from the C-Suite to the End-User

Raising awareness of cyber security is a constant effort which requires participation at all levels and facets of the organization. In conjunction with regular IT security training programs, an Awareness Campaign helps to communicate information security issues and challenges to the user community. This presentation will briefly describe the elements of NASA's Cyber Security Awareness Outreach Campaign and demonstrate how that campaign can lead to increased awareness through improved communication and coordination with everyone from Senior Leadership to the end users.

Valarie J. Burks, Deputy CIO for IT Security, NASA Office of the Chief Information Officer

Valarie J. Burks is the Deputy Chief Information Officer for IT Security at NASA. Since February 2011, Ms. Burks has provided Executive leadership and oversight in the areas of Security Services Oversight and Planning, Security Operations, Governance, Risk, and Compliance, Awareness and Training, Privacy , and IT Security Emerging Technologies. Ms. Burks has made major strides to enhance the NASA IT Security Program instituting changes which defined the strategic and tactical direction for IT Security at NASA, expanded enterprise IT security services and increased collaboration with public and private sector entities.

Previously, Ms. Burks served as the Associate Chief Information Officer for Cyber and Privacy Policy and Oversight at the U.S. Department of Agriculture (USDA) since 2009. She managed Federal Information Security Management Act reporting, governance, risk and crisis management, strategic oversight and compliance. She has a significant backgroundand experience in IT management. Ms. Burks led the development and launch of the USDA Certification and Accreditation Center of Excellence to improve and mitigate system risks, reduce costs and improve the quality and standards for systems.

Ms. Burks also served as Director for USDA's Washington Communications and Technology Services Division since February 2005. She developed, managed, and maintained IT infrastructure and equipment including network, desktop, video, web-hosting and telecommunications operations. Prior to that appointment, she served as Director for the USDA Universal Telecommunications Network (UTN) program. Ms. Burks began her Federal service as an Auditor/Computer Scientist with the Government Accountability Office in 1989. She has more than 20 years of experience leading IT organizations in the Federal and private sector.

Ms. Burks received her Bachelor of Science Degree in Computer Science from the University of Maryland, Baltimore County. She also received her Master of Science Degree in Computer Systems Management from the University of Maryland, University College. In August 2008, Ms. Burks completed the Key Executive Leadership Certificate Program at American University.

Cyber Security Awareness Training in the Age of Mobile Devices

This lecture will reveal the latest threats to information; how the end-user is being targeted; how easy it is to lose or have information stolen in the age of mobile computing; and, what organizations can do to better train employees, get them to care, and create a lasting impact.

The workforce/end-user is the weak link today. Phishing and spam attacks are ever increasing and getting more and more sophisticated because hackers know they can get people to click on anything. The standard power point training is ineffective for lowering the risk of a cyber-attack. Most click through the training as quick as possible hoping to complete the test quickly and move on with their lives having accomplished the annual security training. Training must be captivating, fun, and informative helping employees to understand the current threats to data and how it can impact their lives. Training must emphasize the impact and how employees need to take a greater interest in protecting the information of the organization, client, customer, and the public, as well as their own. The influx of mobile devices and use of social media means the organization has lost even more control over sensitive information, and

opened the door to the organization as never before imagined. Simply implementing technical controls is not enough. IT can no longer do it alone and the average worker now holds as much data and computing power in the palm of his hands as an entire organization did ten years ago. The workforce must be made a pseudo member of the IT/Security team and learn how to protect the organization and their own personal information.

David Willson, Attorney at Law, CISSP, Security +, Titan Info Security Group, LLC

David is a leading authority in cyber security and the law. He is a licensed attorney in NY, CT, and CO, and owner of Titan Info Security Group, a Risk Management and Cyber Security law firm, focused on technology and the law, and helping companies lower the risk of a cyber-incident and reducing or eliminating the liability associated with loss or theft of information. He also assists companies with difficult legal/cyber-security issues. David is a retired Army JAG officer. During his 20 years in the Army he provided legal advice in computer network operations, information security and international law to the DoD and NSA and was the legal advisor for what is now CYBERCOM. He has published many articles, such as, "Hacking Back In Self-Defense: Is It Legal; Should It Be?", and recently, "Cyber War or Cyber Cold War?" His speaking engagements include: the FBI ICCS conf., RSA, CSI, HTCIA, ISSA, FBCINC, the 4th Int'l Cyber Crime Conf., Australia, Cornerstones of Trust, FISSEA, ASIS, and others. He holds the CISSP & Security + certifications and has two LLM's in International Law and in Intellectual Property law. He is a VP of his local ISSA chapter and a member of InfraGard. He was recently quoted in a Fox News Exclusive: http://www.foxnews.com/scitech/2012/01/31/exclusive-wikileaks-to-move-servers-offshore-sources-say/?test=latestnews, and his recent article was published on Fox News: Is the US Already Engaged in a Cyber War?: http://www.foxnews.com/opinion/2012/06/05/is-us-already-engaged-in-cyber-war/

	TRACK 1: Green Auditorium	
3:45 – 4:10 pm	**UMUC Cyber Security "Preparing the Cyber Workforce of the Future" Panel Discussion** **Dr. Jeff Tjiputra, Dr. Amy Harding, Dr. Valorie King, Dr. Richard White, Mr. Ernest E. Rodgers, Cybersecurity Professors, University of Maryland University College**	
4:15 pm	**Prize Drawing – Green Auditorium**	

UMUC Cyber Security "Preparing the Cyber Workforce of the Future" Panel Discussion

The University of Maryland University College (UMUC) is a designated "Center for Academic Excellence in Information Assurance Education" by the National Security Agency and the Department of Homeland Security. Two years ago UMUC, The Undergraduate School revamped its already well-established undergraduate Information Management and Information Assurance curriculum into a powerhouse of undergraduate cybersecurity programs delivered around the world. This initiative was in response to industrial and government organizations needing qualified cybersecurity professionals to meet growing threats, identify vulnerabilities, and improve information system security.

UMUC Undergraduate School meets these challenges by moving students through two programs; 1) the CSIA – Cybersecurity and Information Assurance curriculum, and 2) the CMIT – Computer Information Technology curriculum. Students can take courses in one or both programs along several different tracks emphasizing academics or IT security certification offered by several organizations such as $(ISC)^2$ and CompTIA.

Last year UMUC Undergraduate School moved its 12-week semesters to an 8-week format. This was done to better meet the needs of its diverse student population. All courses are now offered either online or in a hybrid format of online and face-to-face instruction in locations around the world. Current and emerging instructional technologies allow for virtual IT laboratories and simulations to be conducted along with instruction to take place using innovative courseware and videoconferencing capabilities.

Future initiatives are underway to further improve the quality of the UMUC Undergraduate School educational experience. With these improvements and partnerships with industry sponsors, UMUC will remain a premier learning institution for cybersecurity well into the future.

Dr. Jeff Tjiputra, Dr. Amy Harding, Dr. Valorie King, Dr. Richard White, Mr. Ernest E. Rodgers, Cybersecurity Professors, University of Maryland University College

Dr. Jeff Tjiputra is the Academic Director for the Cybersecurity program at The Undergraduate School at the University of Maryland University College (UMUC). He also manages the Computer Networks and Security program at UMUC. He has a Bachelor degree in Computer Science, Master degree in Information Networking and Doctorate degree in Systems Engineering. He has been with UMUC since November 2010. Prior to that he was Chair of the Business and Technology Division at the College of Southern Maryland where he also managed their Information Systems Security program and led the effort to get the program certified under the CAE2YR program.

Dr. Amy Harding started teaching for UMUC in 2010. She started in the Information Systems Management program and moved to the Cybersecurity & Information Assurance program in 2012. She teaches Security Policy Analysis and Evaluating Emerging Technologies – an also serves as the Course Chair for the Security Policy Analysis

course. Dr. Harding earned a DM from University of Phoenix and a MS from Bowie State University. She holds the CIO Certification from the iCollege (National Defense University). Dr. Harding spent 23 years working for the U.S. Army as a Department of the Army civilian.

Dr. Valorie J. King has taught information security and information systems management since 2006. Currently, she is an adjunct assistant professor in the Cybersecurity and Information Assurance (CISA) program in The Undergraduate School at the University of Maryland University College. In addition to teaching both the technical and policy sides of cybersecurity, Dr. King is involved in writing curriculum materials for courses in the major. She also serves as a course chair and faculty mentor. Dr. King's Practitioner Experience includes serving as a Deputy Division Chief (Information Assurance Systems and Software) and as a Department of Defense Office of the CIO IT Policy Analyst (Web policy / security). Her IT consulting engagements have included serving as an IT Strategist, IT Policy Analyst, and Software Engineering subject matter expert for secure networks and systems. She has over fifteen years hands-on Software / Systems Engineering for mission critical systems in secure environments. Her federal sector experience includes: program analysis and evaluation for federal agency CIO organizations (CPIC, IT-300, ITIM, E-Government policy and planning, and IT Governance).

Dr. Richard White has taught data communications and computer security since 2001. As an Adjunct Professor, he started with UMUC in 2007 in the Information Systems Management program. In 2010 he moved to the Cybersecurity & Information Assurance program where he teaches multiple cybersecurity courses, as well as serves as the Course Chair for the CSIA capstone course - Practical Applications in Cybersecurity Management. In addition to teaching for UMUC he also serves as the Chief Information Security Officer for the United States Capitol Police. Dr. White earned a PhD from Capella University and a MS from UMUC. Prior to his employment at the United States Capitol Police he provided systems engineering and information assurance consultation, through Booz Allen Hamilton, for the Intelligence Community, Department of Defense and civilian agencies of the federal government.

Mr. Ernest "Ernie" Rodgers began teaching for UMUC as an Adjunct Professor of Cybersecurity and Information Assurance in 2011. His courses include *Foundations of Cybersecurity* and *Foundations of Information Systems Security*. Ernie received his education from the University of Maryland College Park, University of Maryland University College, and the U.S. Army War College. He is currently completing a Chief Information Security Officer (CISO) certificate through the National Defense University's iCollege located in Washington, D.C.

	TRACK 1: Green Auditorium	
4:15 pm	**Prize Drawing – Green Auditorium**	

Thursday, March 21, 2013 – *"Gov Poster Session is back"*

8:00 – 8:45 am	Registration, Breakfast, and Networking
8:45 – 9:00 am	Morning Announcements Daily Announcers: Track 1: Louis Numkin Track 2: Gretchen Morris
9:00 – 9:30 am	Keynote Address: Green Auditorium **Expanding the Role of Minorities in Cyber Security** Lamont Hames, Chief Development Officer, UNCF Special Programs Corporation

Expanding the Role of Minorities in Cyber Security Education

UNCF Special Programs Corporation (UNCFSP), a 501(c)3 non-profit corporation advises Government and Industry regarding the capabilities of Historically Black Colleges & Universities (HBCU) and Minority Serving Intuitions (MSI) to participate in Government sponsored programs. UNCFSP was founded by UNCF Inc., the nation's largest organization focusing on minority higher education.

UNCFSP fosters opportunities in the Federal sector with HBCU/OMI's unique capacity to educate and train diverse human capital talent. UNCFSP provides capacity building, career, entrepreneurial and economic development opportunities in support of over 300 minority serving institutions (MSI's). The institutions, faculty and students from Minority Serving Institutions (MSIs) rely on our expertise to enable a cross pollination between mission centric federal programs, innovation and *solutions* available from this sector of the higher education community.

UNCFSP's Research and Development Consortium (UNCFSP-RDC) was established to leverage the multi-disciplinary skills and resources of minority higher education institutions to deliver services and participate in Government mission oriented programs. The UNCFSP-RDC advances state-of-the-art skills in fields that are needed to develop and transition new technologies for national defense, homeland security, medicine, energy and space. For example, within UNCFSP-RDC exists several institutions with programs in Information Assurance (IA) and Cyber Security including some with the joint Department of Homeland Security (DHS) and National Security Agency (NSA) Center of Excellence NSA and the Department of Homeland Security (DHS) jointly sponsored Academic Excellence. The goal of these programs is to support and reduce vulnerability in our national information infrastructure by promoting higher education and research in IA and producing a growing number of professionals with IA expertise in various disciplines.

Lamont Hames, Chief Development Officer, UNCF Special Programs Corporation

Lamont Hames was recently appointed Chief Development Officer of UNCF Special Programs Corporation (UNCFSP), a 501(c)3 non-profit corporation that facilitates Government and Industry partnerships with the capabilities of Historically Black Colleges & Universities (HBCU) and Minority Serving Intuitions (MSI). UNCFSP was founded by UNCF Inc., the nation's largest and most effective minority education organization.

In this role he is responsible for overall business strategy and development, organizational leadership, project management, innovation, and assists in resolving complex challenges impacting the HBCU and Minority Serving Institutions (MSI) community. He is expanding the organization's mission by executing results driven strategic partnership agreements with Government, commercial, philanthropic, and non-profit sectors to enable program opportunities in STEM, Public Health, Education, Defense and Small Business & Entrepreneurship.

Over a twenty-year span, Mr. Hames brings a unique combination of executive level Federal government and private industry experience. This allows him the ability and credibility to spearhead initiatives with Federal, Congressional, and Industry stakeholders to enable an inclusive environment that allows HBCU/MSI's to continue thriving in a rapidly changing higher education business and technology marketplace that enables scale, sustainability, and accountability, while achieving results.

Prior to his appointment, Mr. Hames worked over five years in private industry serving in senior level capacities and reported directly to the CEO's of two separate high-tech small businesses in the federal IT, multi-media, and management consulting marketplace. His strategies yielded successful results, customer expansion, and new business accounts with agencies ranging from Department of Transportation, NASA, Department of Justice, FEMA, and United States Postal Service to name a few. As a result, he led and closed over $30M in business awards and maintained excellent customer ratings.

Mr. Hames entered public services thru the Presidential Management Fellow's program and spent fifteen distinguished years rising to the (GS-15) rank of Chief of Staff for the Office of Small and Disadvantaged Business Utilization at the National Aeronautics and Space Administration (NASA). There he designed policy, advocacy, outreach, and public-private sector initiatives to enable NASA's supplier diversity program to achieve a record $3.6 Billion dollars in awards to small and minority owned businesses. Mr. Hames has a Bachelor of Science in Computer Science from St. Augustine's University in Raleigh, NC and a Master of Science in Management Information Systems, from Bowie State University in Bowie, MD.

	Track 1: Green Auditorium
9:00 – 9:30 am	**Creating an Online Cybersecurity Capstone Simulation** Dr. Alan D. Carswell, University of Maryland University College and Jim Cook, UMUC

Creating an Online Cybersecurity Capstone Simulation

The purpose of this panel discussion is to describe the experience of University of Maryland University College (UMUC), in conceiving, designing, and deploying an online simulation in its cybersecurity master's programs.

In an educational setting, a simulation is an attempt to immerse the student in a realistic environment that mimics situations the student will encounter when they graduate. A simulation can be thought of as an implementation of active or experiential learning, where the student takes an active part in their learning and applies what they learn to a new context. Simulations stimulate students' higher level skills, requiring them to develop their critical thinking, judgment, and creativity, skills far beyond a rote recitation of given facts.

UMUC is using a large-scale online simulation of a national environment in its capstone masters-level course. The course (CSEC 670 – Cybersecurity Capstone) has students in both its MS in Cybersecurity and MS in Cybersecurity Policy programs. Both programs were designed to be interdisciplinary in nature, incorporating concepts from technology, law, economics, policy formulation, psychology and other fields.

The culmination of CSEC 670 is the Cybersecurity Capstone Simulation (CCS). The CCS is a large-scale, online, multi-player simulation of a national cybersecurity environment. As deployed in our capstone course, CSEC 670, students are divided into teams representing various sectors of the US economy. The simulation consists of multiple "rounds" played during the semester. Each team

makes decisions about various technological and policy cybersecurity measures in a round. The decisions are input into a large mathematical model which then calculates outcomes of metrics like profits, customer satisfaction, system security, etc. In addition, a Game Master injects events like hacker attacks, worm intrusions, or natural disasters into the simulation to make the exercise more challenging for the teams.

The simulation turned out to be extremely complex. That was a design goal, and we wholly achieved it. With all the possible permutations of decisions, events and outcomes, we did a back-of-the-envelope calculation of the possible branches of the "decision tree." The final number turned out to be some two billion possible permutations.

Of course, with so many possible outcomes there is no one "right" answer or set of perfect decisions. A team could make the most rational and optimal decisions, and yet suffer poor outcomes through little fault of their own. Consequently, we devoted considerable effort to fashioning a grading rubric to assess student performance. Students are graded not only on their outcomes in the simulation, but also to the extent they make and justify rational decisions based on a coherent strategy, and demonstrate teamwork.

Developing the simulation was also a complex process, a year-long effort involving several units within UMUC, a team of subject-matter experts, and an external instructional development firm.

The panel members will consist of individuals intimately involved in the design and deployment of the simulation. They include faculty members who focused on its integration within the course and the cybersecurity programs, and the project manager who oversaw the simulation's development. Each panel member has a unique perspective on the simulation, based on their role in its development.

The simulation was first deployed in the summer semester of 2012. Student reactions to the experience were collected through an online survey and will also be presented.

Dr. Alan D. Carswell, University of Maryland University College and Jim Cook, UMUC

Dr. Alan Carswell has been a faculty member and program director at UMUC for over 20 years. He is currently Chair of the Department of Cybersecurity and Information Assurance at UMUC's Graduate School of Management and Technology. Prior to this, he was Chair of the Information and Technology Systems Department, and has served as Program Director of the Information Systems and Services program, all at UMUC. Dr. Carswell has been involved in and managed the development of numerous information systems projects for public, private, and government sector clients. He holds a PhD from the Robert H. Smith School of Business at the University of Maryland.

Jim Cook is Special Projects Manager in the office of Instructional Services and Support at the University of Maryland University College (UMUC). He has extensive experience in project management with oversight of various distance education projects in higher education as well as corporate training in a regulated environment. Jim has a Master's Certificate in Project Management from The George Washington University and an M.A. in Instructional Systems Development (ISD) from the University of Maryland Baltimore County (UMBC). His areas of interest include project management, curriculum and program design, training and education design, and procedure development.

	Track 1: Green Auditorium
10:15 – 10:30 am (time extended if needed)	**Pecha Kucha (Lightning Round)** Moderator: Moderator: Lance Kelson, Dept of the Interior; Gretchen Morris, DB Consulting/NASA; K Rudolph, Native Intelligence; Joshua Black, Defense Cyber Investigations Training Academy; Kevin Rogers, Cypherpath Pecha Kucha (or PK) means "chit chat" in Japanese. We use the term to describe a session that contains a series of rapid-paced slide presentations that are given by speakers.
10:30 – 10:45 am	**Morning Networking Break - hallway outside Green Auditorium**
10:45 – 11:15 am	**Government Best Practice Poster and Demonstration Session** **Portrait Room – Open 10:30 – 2:10 pm** Susan Hansche, Dept of State/Avaya, Coordinator Participants: o FISSEA Security Contest entries – vote for the Peer's Choice ▪ Gretchen Morris, FISSEA Contest Coordinator o DHS Training Catalog and o DHS NICCS ▪ Peggy Maxson, Shannon Nguyen, Amanda Van Hooser, Patrick Keane, Noel Wray

	○ DHS/State FedCTE Virtual World Classroom ▪ Olivia Morris ○ State Dept COL (Cybersecurity Online Learning) ▪ Tammy Brennan, Mike Petock ○ State Simulated Phishing Exercise ▪ Katherine Zinder Martini ○ Preparing for Security Authorizations in a FedRAMP World ▪ Jim Biggs ○ Dept of Education K2 (ED-Defender Quarterly Awareness Campaign) ▪ Deborah Coleman, Karen Urban ○ SecureIT Day Reminder Campaign Poster ▪ Janet Wilson ○ FedRamp Emerging Technologies (Leveraging the FedRAMP Security Protocol as a Policy and Procedural Model for Emerging Technologies) ▪ Maria Horton
	Track 1: Green Auditorium
11:15 – 11:45 am	**BYOD (Bring Your Own Device) Panel** Loyce Pailen, UMUC Moderator; Tijan Drammeh, Washington Metro; Andrew Gaither, UMUC; Kimberly Hancher, EEOC

BYOD (Bring Your Own Device) Panel

The acronym BYOD, commonly stands for "Bring Your Own Device", and it generally refers to the fact that there is a proliferation of computing devices – laptops, smart phones, tablets etc., owned by employees and business partners that can be brought into the work place for use to connect to the corporate network and can also access corporate date. This recent phenomenon poses several challenges that are sometimes not fully appreciated and discussed, and the repercussions, absence of proper and adequate policies regulating their use, can be severe from a security perspective. On the other hand, BYOD can also improve productivity and be a motivating factor for employees since they will be using devices that they are attached to and are familiar with. These policies have to address the following:

a. Clear goals for a BYOD

b. Identify organizational requirements for mobile connectivity – different organizations have different needs for mobile connectivity

c. Will employee and partner devices be allowed on the corporate internal network

d. Should there be a separate network for BYOD that will not directly interface with the internal network

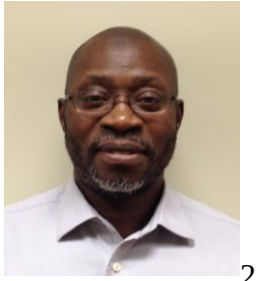
e. What devices and Operating Systems will be supported on the corporate network

f. What additional controls are needed for BYOD – encryption, applications allowed, remote wipe of devices, etc

g. Who dictates the management of these devices outside work

Regardless of what policy stipulations are created, the most important aspect of BYOD is to make sure that it fits the organizational culture. In addition, buy-in must come from the very top of the organization, not just IT. And of course BYOD education and awareness should accompany the technical discussions as well.

Dr. Loyce Best Pailen, Collegiate Professor, University of Maryland University College, Graduate School of Management and Technology, Moderator; Tijan Drammeh, Information Systems Security Officer, Washington Metropolitan Area Transportation Authority; Andrew Gaither, Sr Information Security Analyst, University of Maryland University College; Kimberly Hancher, Chief Information Officer, Office of Information Technology (OIT), Equal Employment Opportunity Commission (EEOC)



Tijan Drammeh is presently an Information Systems Security Officer for the Office of Cyber Security within the IT organization of the Washington Metropolitan Area Transportation Authority (Metro). In this role, he leads the Risk Management group responsible for conducting risk assessments, enterprise vulnerability management, audits and policy development for the entire Metro organization. This role includes responsibility for PCI, Safety and Security and Financial audits conducted by outside auditors as dictated by regulations. Recently, Mr. Drammeh was part of the core team of individuals from WMATA that is

developing and deploying a BYOD program.

Prior to assuming this position, Mr. Drammeh held a variety of positions including Manager Risk & Compliance for UMUC (UMUC is the largest public online higher Ed Institution in the US) and Manager Disaster Recovery for UMUC where he built the BC program.

Andrew Gaither started his career at University Maryland University College (UMUC) in the University's proprietary Learning Management System (LMS) WebTycho in 2005. After serving a variety of roles within IT he moved to UMUC's Enterprise Risk and Compliance in 2012 and in his short tenure he has lessened UMUC risk profile by leading the implementation of a Cloud based DLP and signature less malware defense system.

He serves on the Alumni Board of University of Maryland Baltimore County (UMBC) and serves as President of the UMBC RFC Alumni Association. The RFC Alumni Association is proud to boast of the first athletic club scholarship in UMBC history and its work for providing a network of personal and professional support for recent graduates of UMBC RFC.

Kimberly Hancher began her Federal career at the Department of Veterans Affairs in 1981 and implemented the VA's first enterprise wide electronic mail system. After 15 years at the VA, she joined the Federal Communications Commission (FCC) to lead the electronic government (e-gov) program. During her 10 year stint at the FCC, the agency deployed over 20 public facing, online, web based transaction systems and implemented mandatory electronic filing. She joined the Equal Employment Opportunity Commission (EEOC) as the Chief Information Officer in 2008 and is leading several transformational efforts there. In 2012 the EEOC became one of the first Federal agencies to implement a BYOD pilot program.

She is a valued member of the Federal senior executive service; known for her ability to leverage IT, create a shared vision of the future, and serve as a mentor/role model for aspiring IT professionals. She currently serves as a board member on the Government Information Technology Executive Council (GITEC) and Chair of the ACT/IAC BYOD working group.

Mrs. Hancher is also active in charitable non-profit organizations. She was President and CIO of The Angels Network (www.theangelsnetwork.org), a charitable group that raises funds for transitional housing and homeless programs in the DC metro area. In 2007 she received the President's Volunteer Service Award in recognition of her commitment to community service. If you want to get on her good side, ask her about The Angels Network.

	TRACK 1: Green Auditorium	TRACK 2: Lecture Room B
11:50 – 12:20 pm	**The National CyberWatch Center** Davina Pruitt Mentle, Margaret Leary, PhD, Dr. Costis Toregas, GWU and CyberWatch	**Building the Next Generation of Cyber Defenders: Cross-Training Wounded Warriors to help Protect and Defend the Nation's Information Systems** Jim Wiggins, Federal IT Security Institute and Sam Maroon, Dept of State

The National CyberWatch Center

The National CyberWatch Center, a consortium of 2- and 4-year educational institutions, is an Advanced Technological Education (ATE) National Center, headquartered in the Washington, D.C. region and funded by the National Science Foundation (NSF). This presentation will focus on our mission to increase the quality and quantity of the cybersecurity workforce in the nation. Through our resources, members have access to information assurance/cybersecurity curriculum, program graduates, virtual labs, educational resources (such as the CyberWatch Second Life Island available for hosting training sessions), and professional development opportunities. We will also discuss lessons learned in building a successful collaborative model to build and support a technical cybersecurity workforce. The new National Center goals and capacity building initiative will be shared.

In this session, we will give an overview of a highly successful collaborative model for building cybersecurity workforce capacity and discuss the new mission and goals of the National CyberWatch Center.

Attendees will also learn more about where to access:

- Curriculum
- Resources
- Virtual labs and exercises
- Competitions
- Learning platforms
- PD activities

Davina Pruitt-Mentle, Ph.D., Senior Researcher and Policy Analyst, Executive Director, Educational Technology Policy, Research and Outreach (ETPRO) and CyberWatch; Dr. Costis Toregas, Associate Director GW Cyber Security Policy and Research Institute; Dr. Margaret Leary, CyberWatch

Davina Pruitt-Mentle, a senior researcher and policy analyst at Educational Technology Policy, Research and Outreach (ETPRO) and CyberWatch K12 Division PI, has worked in the field of STEM education & educational and cyber awareness research for over 20 years. She holds a PhD from the University of Maryland in educational technology policy and has spent the past 15 years conducting research on student and educator cyber awareness and K-16 cyber ethics, safety and security educational programs, & developing programs to help increase the IT/IA workforce pipeline. Research and development interests have focused on the Cyberethics, Cybersafety and Cybersecurity (C3) framework and the connection to the broader Digital Literacy landscape. Some of her recent published works have focused on the state of C3 awareness knowledge and programs, cyber awareness strategies, and SECURE IT, a holistic approach program to promote C3 and connect to careers in Cybersecurity. She serves on numerous local, state and national Task Force/Advisory Boards including NetSmartz, iKeepSafe, CLICKS, MD ED Technology, CTE and Technology Advisory Boards, Equity Partnership, ISTE/MSET.

She has served as faculty lecturer within the College of Education at UMCP since 2001, and served as Director of Educational Technology Outreach within the College of Education at UMCP from 2001-2008. Before joining the College, she taught high school Physics and high school and college Chemistry. She also worked as a contractor in the Fuels Science Division at the Naval Research Laboratory. She has acted as consultant to a number of technology and education-related organizations, and has authored and presented at numerous national, regional and state conferences. Dissertation: *Community and Educational Workforce Opportunity in the US: The Relative Utility of Technology and Digital Literacy in a Transcultural Community.*

Dr. Margaret Leary is a Co-Principal Investigator of CyberWatch and full-time faculty at Northern Virginia Community College where she instructs networking and cyber security courses. She also serves as a Senior Security Advisor at Avaya Government Solutions, where she provides security consultation services to several Civilian and Military agencies. Her research interests include identity management and authentication, privacy, and data mining social networking sites. Her other "extra curricular" activities include serving as a Member of the Alexandria City Council IT Commission, Advisory Board Member of Microsoft's Official Academic Curriculum (MOAC), ANSI-BBB Identity Theft Prevention and Identity Management Standards Panel, Member of several ACM Working Groups, and contributor to NIST and other workgroups examining Cloud Security.

Dr. Toregas is the Associate Director of the GW Cyber Security Policy and Research Institute. He is Lead Research Scientist in the GW Department of Computer Science, an adjunct faculty member in the Trachtenberg School of Public Policy and Public Administration at George Washington University (GW), and the Director, Industry Liaison and Sustainability for the National CyberWatch Center, an NSF funded ATE Center focused on workforce development in Cyber Security. He teaches courses in Public Private Partnerships and IT as Empowerment for Public Administrators. His research interests include Computer Security and Information Assurance, the intersect of policy and technology in the public sector, and aspects of Social Equity in public administration.

Professor Toregas led the non-profit Public Technology Inc. organization for more than 35 years, advocating the creation and deployment of new innovative technologies for local governments in partnership with the private sector, and lectures extensively in 6 continents about the impact of the digital age on government. Professor Toregas also serves as the IT Adviser to the County Council of Montgomery County, MD, overseeing the investment of $230m annually in Information Technology goods and services. He is a fellow of the National Academy of Public Administration, and the immediate past chair of its standing panel on Social Equity in Governance. His consulting assignments include a variety of local government management and collaboration efforts in IT Governance and Public Safety. He is an Executive Coach for the Management Directorate of the US Department of Homeland Security, and a Special Initiatives facilitator for the Eye on Earth Summit in Abu Dhabi, UAE.

Dr. Toregas holds Ph.D and M.S. degrees in Environmental Systems Engineering and a B.S. in Electrical Engineering from Cornell University.

Building the Next Generation of Cyber Defenders: Cross-Training Wounded Warriors to help Protect and Defend the Nation's Information Systems

Today's cyber attacks are continuing to become more technically astute and effective. Gone are the days of simple denial of service attacks targeting websites and other Internet-facing IT systems. Today's attacks are targeting the intellectual property and economic foundations of organizations in every industry, vertical and country. The theft of such information is a common occurrence as critical

information systems are infiltrated through Internet connections and vital economic capital, critical technologies, and other forms of national wealth are being plundered.

Real-life events demonstrate that those organizations that employ highly technical cyber security professionals in areas such as incident response, network defense, and penetration testing or forensics analysis are in the best position to identify, quarantine and remediate today's cyber threats. The differentiator is not just a device or appliance. There is a critical need for people who are able to use judgment and analysis at a deep technical level that can make the difference.

The problem for our nation is this: we don't have enough people with the right mix of technical cyber security skills to adequately protect and defend all the information systems.

The need is real. The supply of trained personnel is limited. Something needs to be done. This presentation will discuss an advanced training and assessment program currently in development by the Federal IT Security Institute to arm our wounded warriors with technical skills that supplement their existing dedication, patience, and devotion to duty, thereby strengthening national cyber defenses.

Jim Wiggins, Executive Director, Federal IT Security Institute

Jim possesses over 16 years direct experience in the design, operation, management, and auditing of information technology systems, with the past 12 years focused on information systems security. He has an extensive background in technical education and specializes in security certification courses targeted at federal and government contracting clients.

Additionally, Jim is the executive director of the Federal IT Security Institute (FITSI). FITSI is a non-profit organization that provides a role-based IT security certification program targeted at the federal workforce.

In 2011, the Federal Information Systems Security Educators' Association (FISSEA) named him "Educator of the Year" for the impact he is making in the federal workforce.

Jim holds the following IA/IT security certifications: CISSP,ISSEP, CISM, CISA, SCNA, SCNP, CAP, IAM, IEM, SSCP, CEH, ECSA, CHFI, LPT, TICSA, CIWSA, Security+, and MCSE: Security and FITSP-M.

Samuel A. Maroon, Instructor, Department of State

	TRACK 1: Green Auditorium	TRACK 2: Lecture Room B
12:20 – 1:20 pm	**Lunch Break – NIST Cafeteria Rear** **Visit the Government Best Practice Poster and Demonstration Session Open 10:30 – 2:10 pm**	
1:25 – 1:55 pm	**The Imperative to Customize the Message to the Audience: A Dialogue about the Strategy for Awareness, Education, and Training related to Cybersecurity's Newest Threat, Global Information and Communications Technology Supply Chain Exploitation** Dr. Elizabeth McDaniel and Tom Barth, Institute for Defense Analyses	**The Science Behind Virtualization** Kevin Rogers, CEO and President, Cypherpath *(replacement for Albert Lewis, MITRE)*

The Imperative to Customize the Message to the Audience: A Dialogue about the Strategy for Awareness, Education, and Training related to Cybersecurity's Newest Threat, Global Information and Communications Technology Supply Chain Exploitation

The White House's Comprehensive National Cybersecurity Initiative # 8 specifically calls for education related to supply chain risk management (# 11). With the support of the National Initiative for Cybersecurity Education (NICE), the Department of Defense (DoD) is developing a strategy for awareness, education, and training related to sabotage, espionage, and counterfeits in the global Information and Communications Technology (ICT) supply chain, an emerging national security threat. DoD's strategy for awareness, education, and training will be customized to meet the specific needs of various key audiences, first for DoD but with the wider government workforce in mind.

Developing the strategy begins with determining the core content using clear terminology, and its relevance to various audiences of current leaders, decision makers, and specialists, and those in training to assume these roles in various organizations. Current approaches to identifying audiences include leveraging the relevant KSAs and competencies in the National Cybersecurity Workforce

Framework (NICE), the five roles cited in the *Notional Supply Chain Risk Management Practices for Federal Information Systems (*NISTIR 7622), the thirteen roles in *Managing Information Security Risk (*NIST Special Publication 800-39)*,* and the important players at various phases of the integrated defense acquisition, technology, and logistics life cycle management system.

Knowledgeable and experienced trainers and educators in the audience will be invited to share their approaches and ideas for matching content with audiences.

Elizabeth A. McDaniel and Tom Barth, Institute for Defense Analyses

Dr. Elizabeth A. McDaniel is currently a research staff member at the Institute for Defense Analyses. Dr. McDaniel served as the Dean of Faculty and Academic Programs at the Information Resources Management College, National Defense University from 1999 through 2010. After earning her Ph.D. from the University of Miami in 1978, she began her academic career at the University of Hartford, where she advanced to full professor, and associate vice president for academic affairs. She was an American Council on Education Fellow in the Office of the President at the University of Connecticut in 1989-1990; Executive Provost and Vice President for Academic Affairs at Nova Southeastern University 1995-1998; and Senior Fellow at the American Council on Education in 1998-1999.

Tom Barth is currently an adjunct research staff member at the Institute for Defense Analysis (IDA). Prior to joining IDA Mr. Barth completed 29 years of commissioned service in the U.S. Army. His most recent assignments prior to retiring included Chief of Future Operations, U.S. Army Cyber Command and Associate Dean of Faculty, National War College, National Defense University. Mr. Barth is a graduate of the U.S. Military Academy, The Army's Command and General Staff College's School of Advanced Military Studies, and the U.S. Army War College. He also served as a fellow in the Massachusetts Institute of Technology's Seminar XXI Program from 2008 to 2009.

The Science Behind Virtualization

The 5 tips you need to know during a budget constrained economy.

During this session you will learn about the science behind virtual worlds and virtual networks. Case studies will be presented demonstrating the use of these innovative technologies for potential adoption into your organization.

Have challenges buying, building, and deploying scalable hands on classes? Would you like to eliminate the human capital needed to setup, install, reset and reconfigure your physical labs? Learn how virtual learning worlds produce better results.

Kevin Rogers, CEO and President, Cypherpath

(late replacement speaker for Albert Lewis)

	TRACK 1: Green Auditorium	
1:55 – 2:10 pm	**PM Break hallway near Green Auditorium – last chance to visit Government Poster Session**	
2:10 – 2:40 pm	**Closing Keynote: Wireless Vulnerabilities** Gary Stanley, NSA	

Wireless Vulnerabilities

The wireless vulnerabilities presentation will discuss inherent vulnerabilities that exist in most wireless devices today and will include a live demonstration of how the devices may be exploited.

Gary Stanley, NSA Information Assurance Directorate

Gary Stanley is from the Information Assurance Directorate (IAD) at the National Security Agency (NSA). In his 30 year career at NSA he has spent time in the Technology Directorate as well as IAD serving in various rolls such as System Administrator, Technical Staff Officer and various Leadership positions. Most recently he completed a two year tour at the Department of State as the NSA Senior Information Assurance Liaison.

2:45 pm	**Green Auditorium** **Prize Drawing – Conference Close**

Thank you

- Conference Director: Patricia Toth, NIST
- Conference Coordinator: Peggy Himes, NIST
- **Speakers for donating their time, energy, and knowledge**
- Conference Assistance: (integral to this effort) Art Chantker, Sue Farrand, Susan Hansche, Al Lewis, Gretchen Morris, Loyce Pailen, and Davina Pruitt-Mentle
- Masters of Ceremonies: Louis Numkin, Cheryl Seaman, Gretchen Morris, Art Chantker
- Participants for entering the Security Contest and sharing posters, trinkets, newsletters, websites, and portions of training programs and to Gretchen Morris and Al Lewis for coordinating the contest and special thanks to the impartial judges.
- Participants for sharing their ideas and programs in the second FISSEA Government Best Practice Poster and Demonstration Session and to Susan Hansche for coordinating this event.
- Participants for the Pecha Kucha (Lightning Round) and to Al Lewis for coordinating this event and Lance Kelson for filling in as a replacement moderator.
- FISSEA 2013 Technical Working Group Members for their contributions throughout this past year and serving as the Program Committee: Scott Anderson, Daniel Benjamin, Art Chantker, Terri Cinnamon, Brenda Ellis, Susan Farrand, Ray Greenlaw, Angela Guinn, Susan Hansche, Peggy Himes, Craig Holcomb, John Ippolito, Maria Jones, Lance Kelson, Albert Lewis, Davina Pruitt-Mentle, Gretchen Morris, Loyce Pailen, Cheryl Seaman, Patricia Toth, and Jim Wiggins
- NIST Support: NIST ITL Computer Security Division, Kevin Stine and Judy Barnard.
- NIST Conference Office: Mary Lou Norris and Teresa Vicente. NIST AV technicians.
- American Public University, Dan Benjamin, for attendee bags
- Art Chantker, Potomac Forum, for radio advertising announcements
- Registration Coordination and Vendor Exhibition: Federal Business Council (FBC), Shannon Grady Lee
- Attendee/speaker items from Julia Gagnon, PMSI – Professional Marketing Services
- Prize Drawing Gift Contributors:
    - SANS Institute, Brian Correia - 3 IPADS
    - Potomac Forum, Art Chantker – certificate to training course and miscellaneous prizes
    - Patricia Toth – miscellaneous NIST items

Thank you, Attendees, for coming.