fissea Federal Information Systems Security Educators' Association

A New Era in Cybersecurity Awareness, Training, and Education

25th Annual FISSEA Conference
March 27-29, 2012

www.fissea.org

National Institute of Standards and Technology

100 Bureau Drive, Gaithersburg, MD

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

"A New Era in Cybersecurity Awareness, Training, and Education" - 25th Anniversary

Program

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

Tuesday, March 27, 2012

8:00 – 8:45 am	Registration, Breakfast, and Networking
8:45 – 9:00 am	Conference Welcome: Patricia Toth, NIST, FISSEA Conference Director and Louis Numkin, FISSEA Life Member NIST Welcome: Donna Dodson, Division Chief, Computer Security Division, and Deputy Cyber Security Advisor, NIST
9:00 – 10:00 am	Keynote Address: A New Era in Cybersecurity – What it Means for Practitioners. What it Means for Users. VADM, Patricia Tracey, USN (ret), Vice President, Defense Industry & Development, HP Enterprise Services and RADM Betsy Hight, USN (ret), Vice President, Cybersecurity Practice, HP Enterprise Services

Donna Dodson, Division Chief of the Computer Security Division, the Deputy Cyber Security Advisor, National Institute of Standards and Technology (NIST)

Donna Dodson is the Division Chief of the Computer Security Division, the Deputy Cyber Security Advisor at the National Institute of Standards and Technology (NIST), and the Acting Executive Director of the National Cybersecurity Center of Excellence (NCCoE). As part of the management team, Donna helps direct the development of NIST's standards, technology and research for the protection of information systems against threats to the confidentiality of information, integrity of information and processes, and availability of information and services in order to build trust and confidence in Information Technology (IT) systems. She is also an active contributor in the areas of authentication and cryptography. Donna has also managed programs including the Advanced Encryption Standard, key management, PKI, authentication and security testing.

Keynote Abstract: The New Era in Cybersecurity — What it Means for Practitioners. What it Means for Users.

The ever-evolving nature of the threat coupled with the substantial changes taking place in the way users interact with information technology and the IT dependence of most enterprises create increasing complexity for everyone from SysAdmins to CIOs to users to mission owners. Exploring the ways in which this complexity manifests itself in various roles and responsibilities across the workforce can help guide the development of training and education models and methods suited to the Cybersecurity era we are entering.

Keynote Speakers: VADM, Patricia Tracey, USN (ret.), Vice President, Defense Industry & Development, HP Enterprise Services, and RADM Betsy Hight, USN (ret.), Vice President, Cybersecurity Practice, HP Enterprise Services

U.S. Navy Vice Adm. (Ret.) Pat Tracey *(on left)* is Vice President, Defense Industry & Development, HP Enterprise Services. She is responsible for U.S. defense business strategy development and industry collaboration. Tracey and her team of defense industry experts have the responsibility of expanding opportunities for HP growth in the defense market.

Recognizing a key opportunity, Tracey championed the establishment of a separate Cybersecurity Practice organization and attracted unique talent to strengthen HP's core capabilities and position in the rapidly expanding cybersecurity market.

Prior to joining HP, then EDS, in 2006, Tracey completed a distinguished 34-year career with the U.S. Navy, retiring as vice admiral and the first woman to achieve three-star rank in the military. A native of The Bronx, New York, Tracey was commissioned an Ensign in 1970 and reported for her initial assignment as an orbital analyst and satellite surveillance officer at the Naval Space Surveillance Center.

In operational assignments in the Navy, Tracey conducted shipboard firefighting, damage control, and hull maintenance training as Commanding Officer, Naval Technical Training Center, Treasure Island; homeport operations for the second largest fleet concentration in the U.S. Pacific Fleet as Commanding Officer, Naval Station Long Beach; and as a Flag Officer, commanded the largest enlisted training command including the Navy's boot camp at Naval Training Center Great Lakes. As Chief of Naval Education and Training, she ran a $5 billion global organization of 25,000 employees responsible for all of the Navy's officer, enlisted and foreign military training. She led the successful expansion of the application of information technology to improve the quality, access, effectiveness and cost of Navy training.

Her staff tours focused on ever-increasing responsibilities in strategic planning, systems analysis, force sizing and human capital planning. Over her career, she served on the staffs of the Commander, Pacific Fleet, Chief of Naval Personnel, Chief of Naval Operations, Chairman of the Joint Chiefs and Secretary of Defense, where she served as the Deputy Assistant Secretary of Defense for Military Personnel Policy.

In her final assignment, Tracey became the first Director of the Navy Staff — a 1,400-person headquarters, with nine flag-level directorates responsible for the Navy's $120 billion budget and future force capabilities. Following the 9/11 attack on the Pentagon, which destroyed 89 percent of the Navy Staff spaces, she led the emergency reconstitution effort, taking the staff to wartime footing by midnight after the attack. She then directed design and construction of restored workspaces, bringing the Navy Staff back in the Pentagon for business in 10 weeks.

Following her retirement, she established an independent consulting business focused on systems planning and analysis, governance within the DoD, and professional development of Navy executives. She returned to government service to conduct a strategic review in support of the 2006 Quadrennial Defense Review. Before joining HP, she served briefly as a Senior Fellow at the Center for Naval Analysis.

Tracey serves as a director of the U.S. Steel Corporation and Armed Forces Benefit Association. She is a trustee of Wilson College in Chambersburg, Pa., and represents HP on TechAmerica's CXO Cybersecurity Council.

Tracey's educational achievements include a Bachelor of Arts degree in mathematics from the College of New Rochelle; a master's degree, with distinction, in Operations Research from the Naval Postgraduate School; and a Fellowship with the Chief of Naval Operations' Strategic Studies Group. She also holds an honorary Doctorate of Letters from Wilson College.

U.S. Navy Rear Adm. (Ret.) Elizabeth A. Hight is vice president of HP's Cybersecurity Practice. In this role, Rear Adm. Hight leads a team of cybersecurity experts to deliver strategic, end-to-end cybersecurity solutions to help HP clients anticipate, overcome and reduce security threats and vulnerabilities while achieving their missions. Rear Adm. Hight joined HP in January 2010 as the director of the U.S. Defense Command and Control Infrastructure Practice, which is designed to assist U.S. defense clients in transforming their IT environments.

Previously, Rear Adm. Hight served as the acting Director of Defense Information Systems Agency (DISA) and Commander of the Joint Task Force – Global Network Operations (JTF GNO) from July until December 2009. She served as the vice director of the DISA, a worldwide organization of more than 6,600 military and civilian personnel responsible for planning, developing, and providing interoperable, global net-centric solutions that serve the needs of the President, Secretary of Defense, Joint Chiefs of Staff, the combatant commanders, the Military Departments and other U.S. Department of Defense (DoD) components from April 2007 until her retirement.

Rear Adm. Hight also served as DISA's Principal Director for Operations and Deputy Commander, JTF GNO from 2005 to 2007. As Director of Operations, she was responsible for providing command, control, communications, and computer support to the nation's war fighters. As Deputy Commander, JTF-GNO, Rear Adm. Hight was responsible to United States Strategic Command (USSTRATCOM) for directing the operation and defense of the Global Information Grid (GIG).

Rear Adm. Hight joined the Navy in March 1977. Her first duty station was Naval Communications Area Master Station Western Pacific, Guam, where she was the High-Frequency Receiver Site Division Officer. During her career in the Navy, Rear Adm. Hight served in many roles, including program sponsor for the UHF Satellite Communications Program on the CNO staff, Executive Officer of the Communications Security Material Systems, Assistant Program Manager for the UHF Follow-on communications satellite program and Commanding Officer, Fleet Surveillance Support Command.

In July 1997, she transferred to the Joint Staff/J6 where she served as the Chief, Current Operations Division and then as the Executive Assistant to the Director, C4 Systems. In June 2000, Rear Adm. Hight reported as the U.S. Space Command Liaison Officer to the U.S. European Command, Stuttgart, Germany. In 2001, she reported as the Commanding Officer, November 2010 Navy Computer and Telecommunications Master Station, Atlantic and the Program Manager for all IT in the mid-Atlantic region. She was transferred to the CNO Staff and served as the Director, Net-Centric Warfare from June 2003 until September 2005.

She is a graduate of the Defense Systems Management College, the Naval Post-graduate School with a master's degree in telecommunications systems, and George Washington University with a master's degree in information systems.

	TRACK 1: Green Auditorium The New Era
10:00 – 10:15 am	Morning Networking Break
10:15 – 11:00 am	National Initiative for Cybersecurity Education (NICE) Update - Panel Dr. Ernest McDuffie, NIST, Panel Chair Panelists: Rick Bauer, Cybersecurity Credentials Collaborative C3; Sheila McCoy, AFCEA Professional Development Center; Chris Boyer, AT&T and NCSA Board President

Abstract: National Initiative for Cybersecurity Education (NICE) Update - Panel

The vision of NICE is a secure digital nation capable of advancing America's economic prosperity and national security through innovative cybersecurity education, training, and awareness. The full spectrum of cybersecurity needs are covered under NICE; from raising national awareness among the public about the risks in cyberspace; to developing and maintaining an unrivaled, globally competitive cybersecurity workforce and broadening the pool of skilled and educated workers capable of supporting a cyber-secure nation.

An important aspect of achieving this vision is the establishment of public-private partnerships. Collaboration with groups such as industry consortiums and private sector and non-profit associations and councils will help NICE achieve its goals.

This year has been an exciting time for NICE as the various components of the initiative begin to develop and mature. This panel will focus on public-private partnerships and the NICE initiative. Panelists will represent NICE partnerships at various stages of development; share their experiences; explore ways to improve the process and discuss an integrated, coordinated approach essential to achieving success.

Dr. Ernest McDuffie, NICE Lead, NIST

In early 2010 the National Institute of Standards and Technology (NIST) was selected as the lead agency for the National Initiative for Cybersecurity Education (NICE) and they identified Dr. McDuffie to be the Lead of this important National Initiative. In his previous position he had been appointed the Associate Director of the National Coordination Office (NCO) for Networking and Information Technology Research and Development (NITRD) in February 2008. From early September 2009 until early November 2009 he served as Acting Director of the NCO. His appointment as the Associate Director of the NCO comes after joining the NIST as a Computer Scientist in their Information Technology Laboratory, Office of Federal and Industrial Relations. In August 2006, Dr. McDuffie joined the NCO where he served as the Technical Coordinator for the Cyber Security and Information Assurance (CSIA) Interagency Working Group (IWG), Federal Agency Administration of Science and Technology Education and Research (FASTER) Committee of Practice (CoP), and the Software Design and Productivity (SDP) Coordination Group (CG).

Prior to joining the NCO, Dr. McDuffie served as the Deputy Director of the Office of Naval Research (ONR) – Science and Technology for America's Readiness (N-STAR) Initiative. He served as the Lead Program Director for the Federal Cyber Service: Scholarship for Service (SFS) Program at the National Science Foundation (NSF).

He served as an Assistant Professor at Florida State University in the Department of Computer Science where he taught both graduate and undergraduate courses in CS for seven years. Dr. McDuffie has participated in software engineering projects for the U.S. Air Force, the National Center for Atmospheric Research, the Federal Aviation Administration, Lockheed Missiles and Space Company, Los Alamos National Laboratory, and the National Security Agency. Dr. McDuffie received his Ph.D. and M.S. degrees in Computer Science from the Florida Institute of Technology in Melbourne, Florida.

Rick Bauer, Director of R&D, CompTIA

Rick Bauer directs the new product research and development for skills certification at CompTIA, the world's leading provider of vendor-neutral certifications for the IT industry. Rick brings a career of IT management to these tasks, having served as a technology officer and CIO for a variety of companies, both in corporate and in non-profit contexts. Rick directs the cybersecurity working group for CompTIA, and has authored a variety of works on cybersecurity, training, and security policy matters. Rick also chairs the Cybersecurity Credentials Collaborative, representing all of the vendor-neutral cybersecurity and privacy certifications around the world. Rick has advanced degrees from Harvard, the Wharton Business School, the University of Pennsylvania, and lives in Colorado Springs.

Sheila McCoy, Director, AFCEA Professional Development Center

As director of the Professional Development Center, Sheila oversees all aspects of the courses, from course selection through delivery. Sheila joined the PDC as registrar in November 2008 and was selected as Director in October 2009. She is a retired Navy captain with 30 years of extensive experience in command, control, and communications based on various assignments including serving on the

staff of the Department of Navy Chief Information Officer as the Team Leader for Information Assurance and Privacy. After her retirement from the Navy, Sheila worked with Booz Allen Hamilton as a privacy consultant for Federal Government clients. Sheila has earned an MA in Management and Supervision from Central Michigan University and an MS in Systems Technology (Joint Command, Control, and Communications.)

Sheila has been a member of AFCEA since 1982 and was an AFCEA Senior Military Fellow for a one year assignment. She has also been active in the leadership of the Monterey CA, Dahlgren VA, and Northern VA Chapters of AFCEA. Sheila also served eight years as a Director of Navy Federal Credit Union. Sheila holds several military decorations including two awards of the Legion of Merit and several AFCEA awards.

Chris Boyer, Assist. VP Public Policy for AT&T and NCSA Board President

Chris Boyer serves as Assistant Vice President - Public Policy at AT&T Services Inc. Mr. Boyer's responsibilities include the development and coordination of AT&T's public policy positions on the Federal and state level on issues impacting emerging services and technology including issues related to cyber security.

In this capacity Mr. Boyer serves as AT&T's representative on the board of the National Cyber Security Alliance a public private partnership dedicated to promoting cyber security awareness for home users, small and medium size businesses, and primary and secondary education.

Prior to this assignment Mr. Boyer was AT&T's dedicated public policy resource embedded with AT&T's business units responsible for coordinating the company's nationwide efforts to expand fiber optics into neighborhoods to deliver Internet Protocol (IP)-based television, faster high-speed broadband Internet access and voice services under the AT&T U-verseSM brand. In this role Mr. Boyer has represented AT&T before numerous external audiences and policymakers as a subject matter expert on AT&T's U-verse initiative.

Mr. Boyer joined AT&T in 1993 and has held various positions in AT&T's corporate public policy, network planning and engineering, product marketing and network services departments including extensive experience working on AT&T's broadband, VoIP and IPTV initiatives. Mr. Boyer holds a Bachelor of Science in Business Administration degree from the University of Kansas in Lawrence, Kansas and an MBA from the University of Houston in Houston, TX.

	TRACK 1: Green Auditorium The New Era
11:00 – 11:25 am	The 21st Century Cybersecurity Workforce Framework Margaret (Peggy) Maxson, Department of Homeland Security

Abstract: The 21st Century Cybersecurity Workforce Framework

The Framework defines cybersecurity work and workers according to a common lexicon and taxonomy to provide a means of categorization. This session provides the opportunity for input from and discussion with government, academic and industry cybersecurity thought leaders. The expertise of these individuals is leveraged throughout the entire process in order to provide necessary input to the qualitative data collection activities.

Organizational adoption of the Framework requires that an organization incorporate the NICE specialty areas into its own Human Resources materials, and that it defines cybersecurity roles according to those included in the NICE Framework. Federal agencies should be incorporating the Framework by December 2013. 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 of the NICE Framework in the near future.

Margaret (Peggy) Maxson, Director of National Cybersecurity Education Strategy, Department of Homeland Security

On 19 April 2010, Ms. Maxson was appointed to her most recent position, 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-leading 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 34 years at the National Security Agency in managerial positions in operations, policy, foreign relations, customer service, and technology development.

Ms Maxson has a Bachelor of Arts in Business Management from the University of Maryland. She is a graduate of the 2005-2006 National Security Fellowship Program at Harvard University, where she focused her studies on leadership and international issues.

	TRACK 1: Green Auditorium The New Era
11:25 - 11:45 am	Customizing the Cybersecurity Workforce Framework for Federal Agencies Angela Guinn, Department of Veterans Affairs, Keri Nusbaum, Department of Homeland Security, Susan Hansche, Avaya Gov/Department of State

Abstract: Customizing the Cybersecurity Workforce Framework for Federal Agencies

How does the NICE workforce framework fit in with your agency workforce identification? Is it the same as workforce as the "significant security" workforce? Join us for this panel session to hear the panelists discuss how their agencies are mapping and/or utilizing the NICE framework in their cybersecurity workforce identification plans.

Angela Guinn, Department of Veterans Affairs, Keri Nusbaum, Department of Homeland Security; Susan Hansche, Avaya Gov/Department of State

Angela Guinn, Department of Veterans Affairs

Ms. Angela Seal-Guinn is the Information Technology Workforce Development Supervising Program Lead for the Office of Information and Technology at the Department of Veterans Affairs. A graduate from University of Phoenix, and having over 15 years previous government experience, Angela officially joined the Department of Veterans Affairs in 2006. Since joining VA ITWD, Angela has established a reputation as being an Information Security Policy subject matter expert and has led the innovative development of a practical and effective competency model program. In June 2008, she became a FISMA Fellow and is regularly invited to present at both internal and external IT related conferences. Since joining ITWD, Angela has leveraged her Information Security expertise and acquired hands on experience laying the foundation for various operational training initiatives, including taking the lead on using competency profiles and competency management functionality within the VA's Talent Management System (TMS). Angela, with the support of her team, diligently work to provide specific IT training to VA's 8000+ IT employees and annual Information Security and Privacy awareness training for over 300,000 employees, contractors, students and volunteers throughout VA.

Susan Hansche, Avaya Gov/Department of State

Ms. Susan Hansche, CISSP-ISSEP, is the director of Information Assurance Training Programs for Avaya Government Solutions in Fairfax, Virginia. She has over 20 years experience in the training field and has specific expertise in designing, developing, and implementing Information Assurance and Cybersecurity training programs for Federal agencies. For the past 14 years the focus of her professional experience has been with information system security and building training programs that provide organizations with the skills necessary to protect their information technology infrastructures. An additional expertise is in the understanding of the Federal information system security laws, regulations, and guidance required of Federal agencies. She is the lead author of "The Official $(ISC)^2$ Guide to the CISSP Exam" (2004), which is a reference for professionals in the information system security field studying for the Certified Information System Security Professional (CISSP) exam. Her second book "The Official (ISC)2 Guide to the ISSEP CBK" (2006) is a comprehensive guide to the Information Systems Security Engineering Model for designing and developing secure information systems within the federal government. Ms. Hansche has written numerous articles on information system security and training topics and has given many presentations at conferences and seminars.

Keri Nusbaum, Department of Homeland Security (invited)

	TRACK 1: Green Auditorium The New Era
11:45 – 12:15 pm	National Initiative for Cybersecurity Education Cybersecurity Workforce Inventory Program Dr. Michael Koehler, Department of Homeland Security

Abstract: National Initiative for Cybersecurity Education Cybersecurity Workforce Inventory Program

The National Initiative for Cybersecurity Education (NICE) has tasked the DHS Cybersecurity Education Office (CEO) with assessing and reporting on the current capabilities of the national cybersecurity workforce. Crucial to NICE's support of cybersecurity education and workforce development is an understanding of the current state of cybersecurity workforce capabilities. The intent of NICE's assessment project is to provide the Federal Government with valuable, actionable data that can be used for strategic planning related to cybersecurity human capital. In addition, this information will be used by NICE to identify gaps in cybersecurity workforce capability and, consequently, focus education and development activities to close those gaps.

The foundation underpinning NICE's assessment project is the Cybersecurity Workforce Framework. The project employs a number of data collection vehicles and methodologies to capture the current capability state of the Nation's cybersecurity workforce. This presentation provides an update regarding those efforts and seeks input suggesting improvements to the project and other potential avenues for data collection.

Michael Koehler, Ph.D., Program Analyst, NICE Cybersecurity Workforce Inventory Program Manager, Department of Homeland Security

Dr. Koehler is the Program Manager for the Cybersecurity Workforce Inventory Program, an effort under the auspices of the National Initiative for Cybersecurity Education to collect and report on the capabilities of the Nation's cybersecurity workforce.

His education includes a Ph.D. in Public Administration and Policy and a Master of Public Administration from the University of Georgia, as well as Bachelor of Arts degrees in both Political Science and German from Davidson College.

	TRACK 1: Green Auditorium The New Era	
12:15 – 1:15 pm	Lunch Provided – NIST Cafeteria Rear	
1:15 – 1:45 pm	Presentation of FISSEA Security Contest Winners: Contest Coordinators: Gretchen Morris, DB Consulting/NASA, and Al Lewis, The MITRE Corporation Presentation of 2011 FISSEA Educator of the Year: By Jim Wiggins, Federal IT Security Institute, FISSEA Educator of the Year 2010 to "2011 Winner to be announced at conference"	
	TRACK 1: Green Auditorium The New Era	TRACK 2: Lecture Room B Awareness, Training, and Education
2:00 – 2:25 pm	Leveraging Models from other Professions to Build a Holistic Cybersecurity Education Framework Lance J. Hoffman, Ph. D., Costis Toregas, Ph. D., Diana Burley, Ph. D., The George Washington University	Retool Your Awareness Program to Target User Behavior Shelly Tzoumas, U.S. House of Representatives and Mike Murray, MAD Security

Abstract: Leveraging Models from other Professions to Build a Holistic Cybersecurity Education Framework

As cybersecurity education and workforce development strategies reach maturity, progress in the field necessitates a paradigmatic shift that adjusts the current emphasis from "students as customers" to "society as customers" where individuals charged with the tasks of building and securing software, systems and networks are held to agreed-upon (and enforceable) professional standards (Burley & Bishop, 2011). To that point, cybersecurity is similar to fields such as medicine or engineering where education and workforce development strategies are viewed from a holistic perspective that weaves together curricular standards, licensure and certification requirements, and obligatory continuing education activities in light of a complex, dynamic and somewhat unpredictable environment.

Those addressing the cybersecurity workforce development challenge often reference medical education as a possible cybersecurity education workforce development model (e.g. Burley & Bishop, 2011; I3P, 2011; Evans & Reeder, 2010). The field of cybersecurity today, it is suggested, is akin to 19th century medicine where medical practitioners of the day, who were often self-taught (like many of

today's software developers) and uneven in capabilities, functioned within an emerging field with no (or little) enforceable professional standard for performance. Yet, despite the chorus of suggestions that medical education could serve as a possible model for a holistic view of cybersecurity education and workforce development, the analogy is incomplete and lacking in a number of respects. No one to date has conducted a systematic investigation of the feasibility of leveraging models from medicine or other professions, nor how a holistic framework would manifest in the field of cybersecurity.

The session facilitators have commenced with just such an investigation. Following the lead of the Flexner Report (1910) in medicine and more recent Carnegie Foundation reports on the development of holistic education and workforce development frameworks in several professions (see, for example, reports on educating engineers by Sheppard et al., 2009; and educating lawyers by Sullivan et al., 2007), we begin by defining the current and goal states of cybersecurity education and workforce development.

During this interactive session we will share progress on the investigation of the cybersecurity education landscape, and will invite participants to discuss the feasibility of leveraging educational models from other similarly complex professions (e.g. medicine, engineering) to develop a holistic cybersecurity education and workforce development structure. Based on the discussion of the educational landscape, we will engage participants in a discussion of key questions to support continued investigation. These questions will include:

- Does the academy's conceptualization of what cybersecurity professionals must know and be able to do align with the current and emerging realities of professional practice?
- Is the cybersecurity curriculum organized and delivered in ways that align with what cyber security professionals must know and be able to do now and in the future? And if not, how might it be?
- What professional goals and values might guide the cybersecurity profession in the continuously evolving context? How flexible should these be for various communities, such as different nations?

Lance J. Hoffman, Ph. D., The George Washington University (GW), Costis Toregas, Ph. D., GW, and Diana Burley, Ph.D., GW

Lance J. Hoffman, Ph. D., Director, Cyber Security Policy and Research Institute, GW

Lance J. Hoffman is Distinguished Research Professor of Computer Science and the Director of the Cyber Security Policy and Research Institute at The George Washington University (GW) in Washington, D. C., and the author or editor of numerous articles and five books on computer security and privacy. He directs the Department of Homeland Security, Defense Department, and National Science Foundation computer security "Cyber Corps" scholarship programs at GW; these programs have produced over four dozen federal government experts in computer security, all of whom have a working knowledge of privacy as well.

Professor Hoffman developed the first regularly offered course on computer security at the University of California, Berkeley in 1970 after serving on the Advisory Committee to the California Assembly Committee on Statewide Information Policy. A Fellow of the Association for Computing Machinery, Dr. Hoffman institutionalized the ACM Conference on Computers, Freedom, and Privacy in 1992, and has served on a number of Advisory Committees including those of Federal Trade Commission, the Department of Homeland Security, the Center for Democracy and Technology, and IBM.

Dr. Hoffman received his B. S. in mathematics from Carnegie Mellon University and his M. S. and Ph. D. from Stanford University in computer science.

Costis Toregas, Ph. D., Assistant Director, CSPRI, GW

Dr. Toregas is the Assistant 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 Marketing Director and Industry Liaison for CyberWatch, 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 the consultant for the Working Group on Policy, Governance and Institutional Networking 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.

Diana Burley, Ph.D., Associate Professor, The George Washington University

Diana L. Burley is an Associate Professor in the Graduate School of Education and Human Development at The George Washington University. Her research interests include IT/cyber security education and workforce development, social informatics, and knowledge management. Burley has a PhD in organization science and information technology from Carnegie Mellon University. She is a research scholar in the GW Institute for Public Policy Studies, and a senior research scientist in the GW Cyber Security Research and Policy Institute, and the immediate-past vice chair of the ACM Special Interest Group on Computers and Society. Contact her at dburley@gwu.edu.

Abstract: Retool Your Awareness Program to Target User Behavior

More and more time has been spent discussing security awareness in the past year. This talk will argue that "awareness" isn't the key to solving the problems plaguing security environments; user behavior is all that matters and our paradigm for altering the behavior of our users is flawed.

Ms. Tzoumas will delve into the “how” to Mike Murray’s discussion on focusing on user behavior. Ms. Tzoumas will discuss how to incorporate marketing, training and real security tools in order to change user behavior. She will share her experience educating and informing a population of users and provide tangible tools and techniques employed.

Shelly Tzoumas, U.S. House of Representatives and Mike Murray, MAD Security

Shelly Tzoumas, Information Systems Security Manager, U.S. House of Representatives

As an Information Systems Securities Manager for the U.S. House of Representatives, Shelly Tzoumas helps protect House data and devices by raising awareness about the threat of cyber-attacks and guiding the House community for safe usage.

During the past two years, Tzoumas extended the reach of the House’s annual awareness training from 5 percent to 81 percent of the 12,000 user community, and she helped the House’s District Office Outreach program reach every congressional district during the 111th Congress, a 60 percent increase over prior years. Tzoumas also introduced the House community to National Cyber Security Awareness Month, which features events led by industry leaders from both the public and private sector. These events are widely attended by House Members and staff.

Currently, Tzoumas is implementing the first role-based security training for House IT staff. She conceived and executed a security awareness campaign brand – “Protect Don’t Neglect” – which has been successfully marketed through a cross channel media plan that included Web, social media, and print platforms.

Tzoumas spent the previous six years implementing a Capital Planning and Portfolio Management program for House Chief Administrative Officer’s Office. Before joining the U.S. House, she owned a small business, served as a web site interface designer and training specialist.

Mike Murray, Managing Partner, MAD Security

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.

	TRACK 1: Green Auditorium The New Era	TRACK 2: Lecture Room B Awareness, Training, and Education
2:35 – 3:00 pm	Entry-level Cyber Operations training development – Perspective of Cisco's Job Task Analysis Process James Risler, Learning@Cisco	Impact of Security Awareness Training Components on Security Effectiveness Karen Quagliata, Ph.D., University of Fairfax
3:00 – 3:15 pm	Afternoon Networking Break	

Abstract: Entry-level Cyber Operations training development – Perspective of Cisco's Job Task Analysis Process

Learning@Cisco is in the process of developing a network security operations analyst course that focuses on identifying threats that are already present within corporate and government networks. This session discusses the Cisco Job Task Analysis (JTA) process that Cisco conducted between various internal and external groups who specialize in monitoring and identify these network intrusions. 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 Cisco knowledge in the entry level analyst.

We will discuss the challenges that Cisco faced developing an intrusion analysis course and why this course required a different approach then what we use when we develop our other security courses. Furthermore, we will address what are called domains of expertise. Additionally, we will address how we captured information during the JTA with Cisco's SOC operations team, applied intelligence group, and Cisco's own Product Security Incident Response Team (PSIRT)

Other topics included in this discussion include Cisco's use of mentoring as a part of the learning process in identifying security threats. We will explore questions such as why are PCAPs 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? The concepts learned as a result of the JTA were broader in nature than initially thought and really had to be integrated with the policies and procedures of cybersecurity.

James Risler, Technical Education Consultant, Learning@Cisco

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 18 years of experience in IP internetworking, including the design and implementation of enterprise networks. Prior to joining Cisco Systems, James provided Cisco security training and consulting for Fortune 500 companies and government agencies. He holds two bachelor's degrees from University of South Florida and will be completing his MBA at The University of Tampa in August 2012.

Abstract: Impact of Security Awareness Training Components on Security Effectiveness

Research has shown that implementing awareness training programs will help improve security effectiveness. Training frequency, training method, and training compliance monitoring are all mentioned in the industry body of literature as playing a role in security awareness training effectiveness. However, no known studies have attempted to examine the patterns of association between these three variables and security effectiveness. Using a questionnaire administered to a sample of members from the international professional organization ISACA, this research project attempted to identify the best possible set of variables for an organization to use in order to implement effective security awareness programs. A quantitative correlational/predictive research design was used to examine the patterns of association between the independent variables of training frequency, training method, and training compliance monitoring, and the dependent variable of perceived security effectiveness. Attendees of this presentation will:

- Get a glimpse into what global organizations are doing in terms of security awareness training.
- Get an unbiased insight into how an international research site views security awareness training within their organizations.
- Get a guidepost for what to focus upon for maximum effectiveness when delivering security awareness training.

Karen M. Quagliata, PhD, PMP, IS Security Analyst, University of Fairfax

Karen Quagliata, Ph.D., PMP has worked in the information technology field for 15 years in diverse capacities. Karen currently works within the financial services industry as an information security analyst, specializing in risk management. In addition, she holds a Project Management Professional (PMP) certification, and is a published writer in various industry publications. In 2010 Karen completed her PhD in Information Assurance from the University of Fairfax. Her doctoral research examined key security awareness training variables and their patterns of association with security effectiveness within an organization. Karen's doctoral findings are published in the August 2011 *ISACA JournalOnline,* in the 2011 InformationWeek Report *Strategy: Justifying Security Training,* and in *The Security Journal* (Fall 2011 edition).

	TRACK 1: Green Auditorium The New Era	TRACK 2: Lecture Room B Awareness, Training, and Education
3:15 – 4:05 pm	Securing the Human: Building and Deploying an Effective Security Program – Lance Spitzner, SANS	Security: Don't Forget the People! Ronald Woerner, Bellevue University

Abstract: Securing the Human: Building and Deploying an Effective Security Program

Highlights Version of MGT433 course: Organizations have invested in information security for years now. Unfortunately, almost all of this effort has been focused on technology with little, if any, effort on the human factor. As a result, the human is now the weakest link. From RSA and Epsilon to Oak Ridge National Labs and Google, the simplest way for cyber attackers to bypass security is to target your employees. One of the most effective ways to secure the human is an active awareness and education program that goes beyond compliance and changes to behaviors. In this challenging course you will learn the key concepts and skills to plan, implement, and maintain an effective security awareness program that makes your organization both more secure and compliant. In addition, you will develop metrics to measure the impact of your program and demonstrate value. Finally, through a series of labs and exercises, you will develop your own project and execution plan, so you can immediately implement your customized awareness program upon returning to your organization.

Lance Spitzner, 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.

Abstract: Security: Don't forget the people!

People are and always will be the weakest link in security. Yet, it's an often overlooked topic within security curriculum. You cannot effectively manage security without understanding people. This session will discuss why humans must be a part of the security solution and how that can be effectively accomplished. It will include a short segue on social engineering and how humans can be hacked. The presenter will discuss the importance of influence and persuasion and how anyone and learn to be an affective security leader and coach.

In this session, we will talk about educating students on people skills and all of its components. If we fail to understand people, we fail to properly implement security controls. We need to ensure we're educating others on methods for reaching, persuading, and influencing others at all levels of an organization.

Ronald Woerner, Director, Cybersecurity Studies, Bellevue University

Ron Woerner is a noted speaker and writer in the security industry and the Director of the Cybersecurity Studies program at Bellevue University. He has twenty years of corporate experience in Information Technology and Security, and has worked for HDR, TD Ameritrade, ConAgra Foods, Mutual of Omaha, CSG Systems, and the State of Nebraska. Ron earned his B.S. in Computer Science from Michigan State University and his M.S. in Information Resources Management from Syracuse University. He is a Certified Information Security Professional (CISSP) and Certified Ethical Hacker (CEH). He has also earned the Toastmasters Advanced Communicator and Leader designations. Ron is a security blogger Bellevue University's Center for Cybersecurity Education. He loves to talk to others who are passionate about Security and Privacy.

	TRACK 1: Green Auditorium The New Era	TRACK 2: Lecture Room B Awareness, Training, and Education
4:15 – 4:40 pm	Social Media Security: Protecting Privacy Srini Srinivasan, Texas A and M University	K-12 Cybersecurity Education Programs Davina Pruitt-Mentle, ETPRO/Cyberwatch

Abstract: Social Media Security: Protecting Privacy

Social media is wildly popular today and thousands of new users are joining social networks daily. Many users are focused on communicating with their friends and not seriously consider the security and privacy implications. In this presentation we highlight the various technologies that are available for the consumer in the social media market. Also, we point out where the security and privacy issues arise as users focus on their communication. Our presentation includes discussion on how the social media settings are meant to provide ease of use for the customer. Thus, it becomes the responsibility of the customer to take into account the potential risks associated with privacy violations. Equally important in our discussion is the steps the customer could take to protect the privacy of the information being communicated and know how certain pieces of information are automatically relayed to the other users on the member's circle of contacts. Also, we would emphasize the monitoring tools available for users which would enable them to take some protective measures.

In a brief analysis of the tools available from major social media outlets such as Facebook, Twitter and LinkedIn we will point out what the settings are meant to do and how certain well publicized violations have hurt the reputations of these providers. We will also highlight some best practices for privacy protection.

We studied the social media acceptance in business enterprises by conducting a survey of several businesses. Our study focused on how businesses perceive use of social media in businesses. We found out that many businesses have come to accept that social media is beneficial for the business to use. We will highlight some of the results of this survey in this presentation.

Srini Srinivasan, Professor and Chairman of Technology Studies, Texas A and M International University

S. Srinivasan is Professor and Chairman of Technology Studies at Texas A and M International University. Prior to joining TAMIU he was at the University of Louisville from 1987 to 2010. He started the Information Assurance program at U of L in 2003. This program was designated a National Center of Academic Excellence in IA Education by NSA/DHS. His research interests are in Information Security. He has published several papers in both Mathematics and Computer Science. Currently he concentrates his teaching and research in Information Security related topics involving Social Media, Cloud Computing, RFID and SCADA. He is the recipient of several grants for security related projects. He spent his sabbatical years at GE, UPS and Siemens. He volunteers his time extensively for public education causes.

Abstract: K-12 Cybersecurity Education Programs

Multiple efforts are underway to encourage students to explore cybersecurity careers. What best practices can we extract with regards to informing students, educators and parents about careers in cybersecurity and other Science, Technology, Engineering and Mathematics (STEM) related fields? What roadmaps can be drafted outlining both the resources required and the potential barriers that have to be overcome? Initial results from the *National K-12 Cybersecurity Education Project* Pilot 1 will be shared and related to nationwide efforts to increase the IT/IA workforce.

We will also describe the underpinnings and design of a collaborative project that posits that the structured collaboration framework ETPRO foments may be a necessary component for the field to move beyond our current levels of representation of students in cybersecurity and other STEM fields.

Davina Pruitt-Mentle, Ph.D., Senior Researcher and Policy Analyst, Executive Director, Educational Technology Policy, Research and Outreach (ETPRO) and 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.*

	TRACK 1: Green Auditorium The New Era	TRACK 2: Lecture Room B Awareness, Training, and Education
4:45 – 5:00 pm	DOOR PRIZES	
5:30 pm	Dinner Get Together – Location Dogfish Head Alehouse (across from Main Gate – 800 West Diamond Ave) Sign up at conference. Reservations in NIST FISSEA name. Dinner is Not included in the registration fee.	

Wednesday, March 28, 2012 – Vendor Exhibit Day

8:00 – 8:45 am	Registration, Breakfast, and Networking
8:45 – 9:00 am	Morning Announcements Daily Announcers: Track 1: Cheryl Seaman Track 2: Gretchen Morris
9:00 – 9:45 am	Keynote Address: Green Auditorium Use of Slogans, Images, and Characters in Federal Information Systems Security Education Neil E. Grunberg, Ph.D., Professor of Medical & Clinical Psychology and Neuroscience, Uniformed Services University of the Health Sciences (USU)

Keynote Abstract: Use of Slogans, Images, and Characters in Federal Information Systems Security Education

Information systems (IS) have become central to professional, personal, and social activities in contemporary society. The security of these information systems is essential. The roles, responsibilities, and challenges to provide effective education (E) to users regarding information systems security (ISS) are enormous. Arguably, motivating Federal IS users to practice appropriate ISS is particularly important. This presentation will highlight how slogans, images, and characters have been used to change attitudes and behaviors. The presenter then will lead a group discussion how these approaches might be applied to ISSE and to FISSE.

Neil E. Grunberg, Ph.D., Professor of Medical & Clinical Psychology and Neuroscience, Uniformed Services University of the Health Sciences

Neil E. Grunberg, Ph.D., is Professor of Medical & Clinical Psychology and Professor of Neuroscience at the Uniformed Services University of the Health Sciences (USU) in Bethesda, Maryland, where he helps to train physicians, psychologists, nurses, scientists, and educators to serve in the armed forces, the Public Health Service, or in academic positions. Dr. Grunberg earned baccalaureate degrees in Medical Microbiology and Psychology from Stanford University (1975). He earned M.A. (1977), M.Phil. (1979), and Ph.D. (1980) degrees in Physiological Psychology and Social Psychology from Columbia University and completed Ph.D. training in Pharmacology at Columbia University's College of Physicians & Surgeons. He has published more than 150 scientific papers on stress, substance use and abuse, behaviors related to physical and mental health, and traumatic brain injury. Dr. Grunberg has received scientific contribution awards from the U.S. Surgeon General, Centers for Disease Control, U.S. Food & Drug Administration, American Psychological Association, and Society of Behavioral Medicine. He has received more than a dozen awards for medical school and graduate education and contributions to USU.

Dr. Grunberg is a daily user of information systems in his personal and professional lives, including his role as a U.S. Federal Government employee who depends on information systems to communicate, teach, learn, conduct research, maintain records, analyze data, and for administrative purposes. Dr. Grunberg spoke at the 2009 and 2010 FISSEA meetings. He is pleased to have the opportunity to speak at the 2012 FISSEA meeting about the "Use of Slogans, Images, and Characters in Federal Information Systems Security Education."

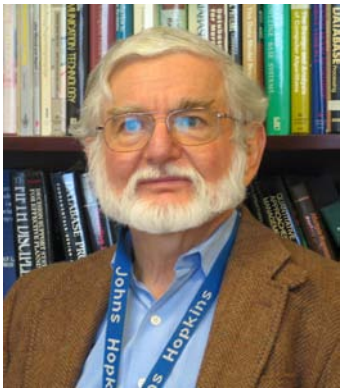
	TRACK 1: Green Auditorium The New Era
9:45 – 10:15 am	Integrating NICE Framework, Assessment and Authorization, and Measurable Security Program Results Dr. George C. Moore, Department of State

Abstract: Integrating NICE Framework, Assessment and Authorization, and Measureable Security Program Results

Traditional security programs are based around inputs, not results. This makes it hard to justify the program and measure its performance. Good training is also based around behavioral objectives – knowing what you want the training to achieve. We discuss how to structure an affordable and effective security program around 15 comprehensive performance metrics, within a maturity model that lets even immature organizations show progress. The metrics demonstrably cover all of NIST SP 800-53 and the SANS 20:

Critical Security Controls. They allow just in time testing placing more emphasis on engineering security in (rather than testing). And, the metrics focus as much on timeliness as completeness. This is a significantly new way to think about a security program. Part of the new model is a focus on continuous monitoring with risk scoring (CMRS) because it has been shown to produce measurable results. We discuss how a good CMRS program is really a (non-traditional) training program, because its purpose is to guide and modify behavior to improve security. A good CMRS program has been shown to measurably improve security. Finally, we show how by mapping the necessary tasks (and related Knowledge, Skills, and Abilities) and controls used to implement the program to a) the 15 metrics, b) the main steps to achieve each metric (sigma-six approach), and c) to their applicable technology, THEN we can build automated tools to let managers build position descriptions that work (and support their program) as well as help employees and trainers identify the training each employee needs. We then use the metrics to measure the impact of training on the program.

Dr. George C. Moore, Chief Computer Scientist, Department of State



Dr. Moore has spent the last ten years working on ways to make security program results measureable, and to use that information to improve security program effectiveness. These efforts have included

- Development and implementation (ISS-LOB) of a "security tips of the day" to provide timely and complete security awareness training (as well as informal training for those with special roles).
- Use of continuous monitoring to decrease security risk (in covered areas) by 90% in one year and sustain this gain.
- Reduction of C&A cost by over 50% sustained for several years.
- Development of a model of how security program effectiveness measures can be used to guide security program architectures, plans, operations, training, etc.

These efforts involve building collaborative teams to bring together people from different disciplines and to integrate political, manager, and operator concerns and abilities. His current work focuses on supporting implementation of these innovations across the civilian sector of the government.

10:15-10:40 am	Morning Exhibit Hall Break: Flag Hallway (Exhibit Hall Open 9:00 – 2:45) The Vendor Exhibit is only one day – Wednesday. Ask FBC for their exhibitor program.	
	TRACK 1: Green Auditorium The New Era	TRACK 2: Lecture Room B Awareness, Training, and Education
10:40 – 11:30 am	Cyber Security, Compliance, Mobility, and Protecting Information David Willson, Esq., Global Knowledge	Bringing Innovation to Security Training – Lance Kelson, Department of the Interior and Shari Hanscomb, DOI

Abstract: Cyber Security, Compliance, Mobility, and Protecting Information

If you are not thinking about how to secure data, especially data on mobile devices and taking action now, consider your organization the next victim of a breach. When that happens, how high is your risk and liability?

Many organizations have already gone mobile but have not seriously considered the risk and adequately trained the workforce. Mobile devices provide a lot of convenience. With that convenience comes many more security holes. What about the BYOD phenomenon?

Last November (2011), the Black Friday reports indicated that the workforce is still doing most of their shopping at work. The only difference now is that instead of using company resources, many are using their mobile devices. Your organization's confidential and proprietary data is seriously at risk, so don't wait to get serious about Mobile security. And, I don't mean just a firewall, anti-virus and anti-malware.

This discussion explores the threats to data, the techniques used, how mobile devices have increased the threat and number of techniques, and the increased risks and liability organizations are facing. The discussion then moves to what organizations can do to be more secure and embrace the mobile device phenomenon through well drafted policies and training, training, training. Learn how to lower risk and eliminate liability.

Major learning objectives include: risks to data, how hackers are getting in, what they are stealing, and some tips on how to better secure and reduce risk and liability.

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

David Willson is owner of Titan Info Security Group, LLC, providing enhanced cyber security and liability reduction or elimination for clients. David is a retired Army JAG officer and a Global Knowledge Instructor. During his 20 years in the Army, he provided legal advice in computer network operations and information security and international law to the DoD and NSA. He was the legal advisor for what is now CYBERCOM. Additionally, he spent half his career as a trial attorney prosecuting and defending. He has published numerous articles, the most recent, *Hacking Back In Self-Defense: Is It Legal; Should It Be?,* and another popular one, *When Does Electronic Espionage Become An "Act of War"?* His speaking engagements include: the FBI ICCS Conference, RSA, CSI, HTCIA, ISSA, FBCINC, the 4th International Cyber Crime Conference, Australia, Cornerstones of Trust, and others. David is a licensed attorney in Co., N.Y., and Ct., and holds the CISSP & Security + certifications. He has two LLM's in International Law in Intellectual Property law. He is VP of his local ISSA chapter and a member of InfraGard. David was recently interviewed by Fox News for an Exclusive on WikiLeaks: http://www.foxnews.com/scitech/2012/01/31/exclusive-wikileaks-to-move-servers-offshore-sources-say/?test=latestnews

Abstract: Bringing Innovation to Security Training: Information Security for Department of the Interior Acquisition Managers

A demonstration of an innovative online Role Based Security Training course for procurement professionals that delivers content-based content for a specific role (CO, COR, PM, etc.).

DOI set out to change the way DOI Contracting Officers, Contracting Officer's Representatives, Program Managers, and Subject Matter Experts buy things that impact security on any level. Our challenge as developers… tailor, target, and deliver instruction that affects the needed change for DOI.

The Team: The DOI Instructional Design Team collaborated with DOI security and acquisition subject matter experts to craft an interactive targeted learning experience.

The Approach: Provide learners only the instruction they need for their unique role and acquisition complexity through on-demand delivery for their customized profile.

The Result: The finished product leverages an engaging avatar coupled with role based variables to tailor the acquisition and role specific instruction and scenarios, resulting in a "choose your own adventure" model!

Lance Kelson, Department of the Interior (DOI) and Shari Hanscomb, DOI

Lance Kelson, Information Security Training Program Manager, OCIO/Information Assurance Division, Department of the Interior

Lance Kelson is currently the Department of the Interior (DOI) information security training program manager and an Adjunct Associate Professor teaching a graduate Information System Security course for Webster University on-site at Bolling Air Force Base. He holds Project Management Professional (PMP), Certified Information System Security Professional (CISSP), Certified Secure Software Lifecycle Professional (CSSLP), and CompTIA Advanced Security Practitioner (CASP) certifications. Mr. Kelson earned a Bachelor of Science in Industrial Engineering at Arizona State University and a Master of Business Administration at the University of Rochester.

Shari Hanscomb, Project and Operations Manager, Office of Strategic Employee and Organizational Development, Department of the Interior

Shari Hanscomb is the Operations and Project Manager for the Department of the Interior's Learning Technology Solutions Division. She has worked for Interior since 2002 and works closely with the Instructional System Design staff to produce innovative online courses for DOI. Shari has her Master's in Management with a concentration in Project Management, and is PMP certified.

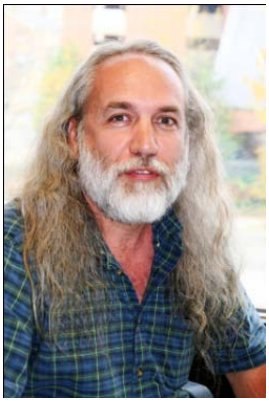
	TRACK 1: Green Auditorium The New Era	TRACK 2: Lecture Room B Awareness, Training, and Education
11:35 – 12:00 pm	Merger Mania: The Mash-up of Security Training at the Financial Management Service (FMS) and Bureau of the Public Debt (BPD) – David Kurtz, Treasury Department, Financial Management Service	USSTRATCOM Cyberspace Training Initiative User Awareness Pilot Program – Tim Kemper, USSTRATCOM (To be presented by Liz Craven, USSTRATCOM/BAH)

Abstract: Merger Mania: The Mash-up of Security Training at the Financial Management Service (FMS) and Bureau of the Public Debt (PPD)

The Treasury Department approved a plan to merge the IT organizations of both the Bureau of the Public Debt (BPD) and the Financial Management Service (FMS), in part as a way to reduce data centers and subsequent costs. In this era of reduced budgets, other agencies may also be looking to merge organizations, so perhaps our experience may be enlightening. One result of our merger has been that the security training programs which had separately evolved at each agency are now trying to unify. It has been surprising to see the number of differences between the two organizations and how they approach security training. Both organizations had been compliant with federal regulations, but often took different paths to get there. Examples of issues that we are dealing with include:

- The mandatory Treasury Cybersecurity tutorial (the civilian version of the DoD ISS-LoB on-line class) had been rolled out in a slightly different format in each organization. One difference was whether it was better to offer a longer window for completion, or focus on a narrower range of dates? The method of follow-up to ensure 100% compliance also differed.
- Specialized security training requirements had also been coordinated differently in each organization. One organization focused more on SkillSoft on-line training classes as a first resort, while the other considered them more as a last resort. Identifying who qualifies as needing specialized security training also was handled differently, as was the process for determining whether a class should count as specialized training.
- Orientation for new employees at the two organizations covered different topics. This happened in part because one organization was allowed 50 minutes to cover security topics the first day, while the other organization was only given 15 minutes.
- The Rules of Behavior were written quite differently at the two organizations. Since the Rules of Behavior are an important component of security training, an effort is underway to derive a new version of the rules for use in both places, which all employees will need to sign.
- One organization was meeting all the requirements for its security training program. The other organization had a history of doing more than the minimum requirements for its program, and had established a tradition of doing so since the '90s. Reconciling the two different programs is difficult because of the vastly different cultures each organization possesses. At one organization, the employees are accustomed to multiple communications about security issues, but transferring that interest and acceptance to a new organization is not easy.

David Kurtz, U.S. Treasury Department, Financial Management Service



David Kurtz now works for the Treasury Department's Financial Management Service (FMS), thanks to a merger six months ago between the IT offices at FMS and his previous employer, the Bureau of the Public Debt. His federal career began as a Presidential Management Intern at NASA Headquarters in Washington, DC. He worked about three years in DC before transferring to Public Debt in his native state of West Virginia 24 years ago. David has worn a number of hats over the years (including work in personnel, EEO, disaster recovery, audit coordination, quality assurance, and mainframe operations) but has been in the security field since 2002. His posters won FISSEA awards in 2006, 2007, 2010, and 2011; he submitted the winning FISSEA logo design; he has written articles for the FISSEA Newsletter; and in 2008 he was recognized as the FISSEA Educator of the Year. He has a B.A. in Political Science from the University of Charleston, and both a Master's in Public Administration degree and a Doctorate of Jurisprudence degree from West Virginia University.

Abstract: USSTRATCOM Cyberspace Training Initiative User Awareness Pilot Program

As military systems and operations become more interconnected and dependent on cyberspace and DoD personnel are increasingly becoming cyber targets, the DoD must develop a robust cyber training program and provide the necessary environment to train cyber-savvy users. USSTRATCOM Joint Exercises and Training Directorate (J7) in collaboration with US Cyber Command J7, US Joint Forces Command J7, and other key training partners completed a comprehensive analysis of cyberspace education, training, and

exercises and developed a Joint Cyberspace Training Plan (JCTP). The JCTP takes into account a model based on several enabling activities to include: education; user awareness; joint cyber exercises and war gaming; large-scale cyber training events; cyberspace modeling and simulation capabilities; virtual environments (cyber ranges); network defense; red teams; and metrics and lessons learned integration.

This presentation focuses on the user awareness enabling activity. The user awareness goal is to successfully change the cyberspace culture and conduct of USSTRATCOM personnel to practice cyber vigilance as a second nature behavior. To do this, the user awareness team has developed a pilot program at USSTRATCOM that focuses initially on the general user and Senior Leadership and is modeled on a change management strategy to measure the deltas of knowledge, performance and motivation of first line defenders by providing continuous improvement {aka cyber security information on a recurring basis}. This presentation highlights insights gleaned from initial analysis, discusses how the insights were applied to the JCTP, and summarizes the key metrics used to assess and measure the success of the training activities and actions being implemented during the USSTRATCOM CTI User Awareness pilot program.

Timothy J. Kemper, USSTRATCOM

Tim Kemper is one of two co-leads for the Cyber Training Initiative (CTI), a joint effort between USSTRATCOM, USCYBERCOM, and Joint Staff J7 Joint Coalition and War-fighting. He has been co-leading this project since October 2010. His team has been tasked with integrating cyberspace operations into DoD training programs across the Joint Learning Continuum. Since his appointment within CTI, Mr. Kemper has led his team to developing six major focus areas or components of the effort, including cyber force development and cyber learning, cyber exercise development, modeling and simulation, cyber training events, network defense, metrics collection and return on investment analysis.

Mr. Kemper led his team to establish requirements for cyber training and commissioned a mobile training team to train combatant commands how to integrate cyberspace operations into their OPLANS and CONOPS. His team is also working on a user awareness pilot with several DoD agencies to change the culture of the general user. Finally his team was instrumental in establishing and executing CYBER FLAG 12. Mr Kemper has his BS degree in Business Administration – Management and is currently finishing his PMP certification through Stanford University.

12:00 – 1:30 pm	Dedicated Exhibit Hall Hours - Flag Hallway (Exhibits open 9:00 am – 2:45 pm) Lunch Provided – NIST Cafeteria Rear	
	TRACK 1: Green Auditorium The New Era	TRACK 2: Lecture Room B Awareness, Training, and Education
1:30 – 2:20 pm	Are We Heeding the Warning Signs? The Federal Cybersecurity Shortage and Skills Gap Panel – Marc Noble, (ISC)² (moderator); Corinne Cook, GIAC; Ron Hale, ISACA; Rick Bauer, CompTIA; Dan Callahan, EC Council	Radio Frequency Identification Devices (RFID) & Near Field Communication (NFC): Two New Threats – Dr. Paul F. Krasley, Defense Intelligence Agency (DIA), National Security Agency (NSA), Unisys

Abstract: Are We Heeding the Warning Signs? The Federal Cybersecurity Shortage and Skills Gap Panel

Companies and governments across the globe are struggling to meet the need for, to locate, hire and retain qualified information security professionals. According to the 2011 (ISC)² Global Information Security Workforce Study released at RSA 2011, Frost & Sullivan estimated that there were 2.28 million information security professionals worldwide. This figure is expected to increase to nearly 4.2 million by 2015 with a compound annual growth rate (CAGR) of 13.2 percent. Further, the Study anticipates the number of U.S. federal information security specialists to grow from 27,000 employees in 2010 to over 61,000 employees by 2015.

The Study also revealed a clear gap in skills needed to protect organizations, resulting in an over-extended cyber security workforce that is showing signs of strain, with new threats stemming from mobile devices, the cloud, social networking and insecure applications, as well as added responsibilities, such as protecting corporate reputation, end-users and customers. And with end users now in the security driver's seat, there is a clear gap in skills needed to protect organizations from these increasing threats from these new technologies being widely adopted by businesses and government agencies.

In an effort to help stem this personnel and skills shortage, cohesion among industry players is a critical element that has been missing – until now.

CompTIA, the EC Council, ISACA, (ISC)², ISSA and SANS, all leaders in IT certifications for more than 25 years, have formed the Cybersecurity Credentials Collaborative (C3), to be announced at RSA Conference USA 2012, to create a sea change in the thinking about solving the skills gap and workforce shortages through attracting, retaining, and educating cyber security experts.

The Collaborative is focused on developing a unified approach among government and industry that marries the ideas and viewpoints of all stakeholders, including cybersecurity education groups, certification bodies and their members, professional groups, cybersecurity innovators, academia and legislators.

The federal information security community is facing a significant transition as pending legislative reform re-defines the national strategy to secure cyber space. Educators won't want to miss this heated yet informative debate on the best solutions to overcome these challenges that impact us all.

Marc Noble, (ISC)2, (moderator); Corinne Cook, GIAC; Dan Callahan, EC Council; Ron Hale, ISACA; Rick Bauer, CompTIA

Marc Noble, CISSP-ISSAP, CGEIT, CISM, NSA-IAM, Director of Government Affairs for (ISC)2 and Co-Chair (ISC)2 U.S. Government Advisory Board for Cyber Security

Mr. Noble is currently the Director of Government Affairs for (ISC)² where he is responsible for advancing the professionalization principles of (ISC)² and increasing the organization's impact, overall reputation and prestige throughout the U.S. federal, state and local government markets. Prior to his role at (ISC)², Mr. Noble worked as an Information Assurance Engineer for MITRE Corp., and held the offices of Chief Information Security Officer and Deputy Chief Information Officer at the U.S. Federal Communications Commission. Over the course of a 30-year government career, Marc also served as Senior Information Security Analyst, Administrative Office of the U.S. Courts and as a Management and Systems Analyst at the U.S. General Services Administration. He holds received his B.A. History/Political Science from Virginia Commonwealth University and a Master's Certificate in Project Management from George Washington University.

Corinne Cook, GCIH, G2700, GCSC, CISSP, GIAC Technical Director

Corinne Cook is a Technical Director with GIAC - a leader in certifying hands-on skills in many key areas of computer, information and software security - where she is responsible for exam content development, relevance, and quality. Corinne has over 13 years of experience in IT and Information Security. Prior to GIAC, she worked in various information security, consulting, and IT administration roles providing support and expertise to public, private, financial services, government, and healthcare related organizations.

Dan Callahan, Director, Federal & Enterprise Affairs, EC Council

Dan Callahan is the Director of Public Sector and Enterprise Affairs for EC-Council. He is the primary liaison with Government/Enterprise wide programs and collaborates with other security certification partners, academia, and EC-Council Authorized Training Centers (ATC). Dan focuses on alliance partnerships that can help individuals, industry, and world wide Governments gain a clear career mapping to industry wide accepted credentials; such as formal education, training, and certification.

As the Program Director of Global CyberLympics Organization Committee, Dan's primary role is to ensure and execute the shared vision of the Organization Committee. Dan will interface with media, alliance partnerships, and other associations who wish to support and participate in the Games. Dan has over 15 years experience in the Training and Education Industry working for organizations that focus on Information Technology, Business Management, and Cybersecurity. His experience crosses both Public and Private sectors in various roles including; Business Development/Sales, Sales Management, Channel Management, and Research.

Ron Hale Ph.D., CISM, Chief Knowledge Officer, ISACA

Dr. Hale is a Certified Information Security Manager with more than twenty years security experience that touches almost every aspect of the security profession. He was the manager of security services for Northrop Corporation Defense Systems Division responsible for developing and managing the security program for classified and unclassified systems as well as corporate investigations, crisis management, technical surveillance countermeasures, executive protection and security awareness. As a research manager for Bank Administration Institute Dr. Hale published research reports on bank security and fraud, and worked on the first study of ATM Security and Fraud. Dr. Hale has also provided consulting services to many leading organizations as a Practice Director in the Enterprise Risk Management practice within

Deloitte & Touche. As part of the ISACA management team Dr. Hale has been responsible for directing the Certified Information Security Manager certification program and for serving the needs of the security profession through research projects and publications. He currently is responsible for leading the research and knowledge product development efforts at ISACA. Dr. Hale has a masters degree in Criminal Justice from the University of Illinois and a doctorate in Public Policy from the Walden University School of Public Policy & Administration.

Rick Bauer, Director of Research & Development, Skills Certification Division, CompTIA

Rick Bauer directs the new product research and development for skills certification at CompTIA, the world's leading provider of vendor-neutral certifications for the IT industry. Rick brings a career of IT management to these tasks, having served as a technology officer and CIO for a variety of companies, both in corporate and in non-profit contexts. Rick directs the cybersecurity working group for CompTIA, and has authored a variety of works on cybersecurity, training, and security policy matters. Rick also chairs the Cybersecurity Credentials Collaborative, representing all of the vendor-neutral cybersecurity and privacy certifications around the world. Rick has advanced degrees from Harvard, the Wharton Business School, the University of Pennsylvania, and lives in Colorado Springs.

Abstract: Radio Frequency Identification Devices (RFID) & Near Field Communication (NFC): Two New Threats

There are two new threats. Radio Frequency Identification Devices (RFID) and Near Field Communication (NFC). Using these two technologies, your professional and private information encoded on your credit cards, community badges and CAC can be read without your knowledge. This session will demonstrate the ease of using RFID and NFC to read your cards from within your pockets or purse and what you need to do to protect yourself. Desired learning outcomes: Awareness and prevention of a new threat.

Dr. Paul Krasley, CPLP, Counterintelligence and Security, DIA

Dr. Paul F. Krasley is an education, training, awareness, and performance improvement professional who for the past 35 years has focused on increasing staff performance using project and program leadership, and training and development in both national and international implementations. Dr. Krasley has developed and implemented projects and training programs as an engineer, director, and vice-president using instructional system development (ISD) for e-learning, computer based, and virtual reality programs in the commercial, State and Federal government environments. Dr. Krasley has a Bachelor of Science Degree in Human Resources Management and Labor relations, a Master's degree in Instructional Technology and a PhD in Education in Training and Performance Improvement. Dr. Krasley is certified by the American Society for Training and Development (ASTD) as a Certified Professional in Learning and Performance Improvement (CPLP) and can be reached at pkrasley@cox.net.

2:20 – 2:40 pm	Afternoon Exhibit Hall closes at 2:45pm / Break – Flag Hallway

	TRACK 1: Green Auditorium The New Era	TRACK 2: Lecture Room B Awareness, Training, and Education
2:40 – 3:05 pm	**Insider Threat** - Tara Mahoutchian and Michael Gelles, Psy.D., Deloitte Consulting LLP	**Professionalization for the Nation** – Angela Curry, National Cyber Security Division (NCSD), U.S. Department of Homeland Security (DHS)

Abstract: Insider Threat

People are an organization's greatest resource, yet, at times, they can also pose a significant threat to its mission and operations. For an organization executing a complex and politically visible mission, the potential loss of confidence in public support at the hands of an employee undermines the agency's ability to execute the mission, recruit staff, and develop sustainable partnerships with other U.S. and international agencies. An initial challenge for most organizations is to understand and define the risks associated with potential breaches of security, including agents assisting in illegal border crossings or allowing other illegal activities, either through willingness or complacency. A secure workforce is the most viable solution to mitigating and managing compromises at any level by employees of the organization, who, both intentionally and unintentionally, exploit assets and mission objectives. Addressing physical and information security through technology comprises only two-thirds of the necessary equation for protecting against asset loss. The third part of the equation, managing a secure workforce and mitigating the threat posed by the vetted employee or the 'insider' is often the most critical variable.

The findings from various studies conducted by the U.S. Government are consistent when referring to the behavior and actions of the 'insider.' The actions that are taken are not impulsive, but intentionally pursued over an extended period. They are often the end result of a complex set of problems, conflicts, and disputes, or a crisis in the individual's personal life. In many cases that means obtaining money, validation, or empowerment. Few entered their organization with the specific intent to violate a trust or facilitate the loss of the organization's assets. Therefore, the motivation to violate trust occurred after they were vetted and hired and while they were already employed and had authorized access to information.

In all cases, insiders engaged in a pattern of behavior that reflected a movement from having an idea to taking an action, all in the service of some solution to a problem. The patterns include: irresponsible handling of classified or proprietary information; irresponsible use of information systems; disclosure or dissemination of information determined to be proprietary or classified to persons without clearance or purpose to have the information; removal of proprietary or classified information or material from secure areas, often taking it home or inappropriately placing it in an open information system; and providing information to others for purposes of facilitating their actions for personal gain or vengeance against perceived wrongdoings by an agency. In almost every case, these activities, if recognized by a vigilant workforce and reported to management, could have been easily interrupted. Additionally, one of the most frequently offered rationalizations by violators is that no one notices, and that physical and information security was lax; if tighter, it would have been more of a deterrent. The lesson learned is that identifying indicators and patterns of at-risk behavior prior to hiring someone and watching for them while an individual works for the organization is a step towards a secure workforce.

Tara Mahoutchian, Deloitte Consulting, LLP and Michael G. Gelles, Deloitte Consulting, LLP

Tara Mahoutchian, Senior Consultant, Federal Human Capital, Deloitte Consulting, LLP

Tara Mahoutchian is currently a Senior Consultant with Deloitte Consulting LLP's Federal practice in Washington, D.C., consulting in the areas of human capital management, organization and talent. She serves clients ranging from the Department of Health and Human Services to the Department of Homeland Security. Her areas of expertise include cybersecurity communications and workforce planning, cybersecurity learning and development, and insider threat.

Prior to joining Deloitte, Tara spent over six years in the commercial sector consulting Fortune 500 clients on recruiting, hiring, and retention best practices and processes. She primarily served the highly regulated telecommunications industry and focused on aiding organizations secure their systems through their human resources. She helped clients determine whether they had the right staff in place to handle sensitive and strategically critical positions and redesigned recruiting and hiring process to attract new talent.

Tara received her Bachelor of Arts in Business Management from North Carolina State University and her Masters of Business Administration from the Fuqua School of Business at Duke University.

Michael G. Gelles, Psy.D., Director, Federal Human Capital, Deloitte Consulting, LLP

Dr. Michael Gelles is currently a director with Deloitte Consulting LLP's Federal practice in Washington, D.C., consulting in the areas of human capital management and systems and operations. Previously, he was the chief psychologist for the Naval Criminal Investigative Service (NCIS) for more than 16 years. He was the lead psychologist for the behavioral consultation team for the Criminal Investigations Task Force, and a member of numerous other task forces in the areas of workplace violence, insider threat and ethics in consultation to national security. Prior to joining the NCIS in 1990, Dr. Gelles served as a clinical psychologist for the U.S. Navy. He is active in a number of professional organizations, including the American Psychological Association Division of Police Psychology, the International Association of Chiefs of Police, the Psychology Services Section, the Society of Police and Criminal Psychology, and the Association of Threat Assessment Professionals. Dr. Gelles is also a frequent lecturer and has published numerous professional papers on topics related to organizational management in operational settings, forensic psychology, law enforcement, terrorism and counterintelligence.

Dr. Gelles received his Bachelor of Arts from the University of Delaware and his master's and doctorate degrees in psychology from Yeshiva University in New York. He completed his clinical and forensic training at the National Naval Medical School and his advanced training at the Washington School of Psychiatry. He held academic appointments in psychiatry at the Uniformed Services University of the Health Sciences and at the Washington School of Psychiatry.

Abstract: Professionalization for the Nation

The National Initiative for Cybersecurity Education (NICE) is a nationally coordinated effort focused on cybersecurity awareness, education, training, and professional development. It seeks to encourage and build cybersecurity awareness and competence across the nation and to develop an agile, highly skilled workforce capable of responding to a dynamic and rapidly developing array of cyber threats.

The goal of Component 3 is to develop a cybersecurity workforce structure strategy to include professionalization, workforce planning, and recruitment and retention. The Cybersecurity Professionalization Analysis project is to deliver a methodology for identifying cybersecurity areas for professionalization.

The *Fontana Dictionary of Modern Thought* defines professionalization as, “a profession arises when any trade or occupation transforms itself through the development of formal qualifications based upon education, apprenticeship, and examinations, the emergence of regulatory bodies with powers to admit and discipline members, and some degree of monopoly rights.”

This talk will provide a brief overview of the project, along with the initial research performed on potential professionalization processes, and the impacts of each by examining the history and procedures of occupations which have professionalized.

Angela Curry, Director, National Cybersecurity Workforce Structure Strategy, Department of Homeland Security (DHS)

In April 2011, Ms. Curry was appointed to her most recent position, Director, National Cybersecurity Workforce Structure 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 leading the workforce structure component of the initiative. DHS requested Ms. Curry for this position following her previous position as the Signals Intelligence Directorate Deputy Chief of Staff for Leadership and Workforce Development, at the National Security Agency (NSA). In this position she led the development of the SI Directorate’s Talent Management Strategy which overhauled hiring and professional development plans by incorporating both qualitative and quantitative assessments in hiring and advancement of the SIGINT professionals.

Ms. Curry has a Master’s of Science in Human Resource Development with a concentration in Organizational Development from Webster University. She has also completed numerous senior leadership development courses and seminars to include Leadership for Senior Executives at Harvard University, and The Government Affairs Institute at Georgetown University.

Ms. Curry served 20 years on active duty in the United States Air Force as a Russian language analyst, strategic analyst, and in a myriad of managerial positions. She spent a year in private industry as a business process re-engineer and was hired as a strategist at NSA in 2003. Ms. Curry has served in a diverse range of leadership and strategic positions in both the Signals Intelligence and Information Assurance missions. She is the recipient of numerous awards and military decorations to include the Defense Meritorious Service Medal, and the Meritorious Service Medal.

Ms. Curry is a new resident of Washington, DC, and has two children. Jefferson is a Combat Medic in the United States Army with the 1st Cavalry Division, deployed since July 2011. Jerrid is a senior at The Barrie School in Silver Spring, MD and hopes to be accepted into the Naval ROTC program in college.

	TRACK 1: Green Auditorium The New Era	TRACK 2: Lecture Room B Awareness, Training, and Education
3:15 – 4:05 pm	A "New" Paradigm: How Community Colleges are Meeting Cyber Workforce Training Needs – Carrie Leary, Margaret Leary, and Costis Toregas, CyberWatch	IT Competency Modeling: Linking the Right People to the Right Training – Terri Cinnamon, Office of Information Technology, Veterans Affairs and Julie Wasielak, Booz Allen Hamilton

Abstract: A "New" Paradigm: How Community Colleges are Meeting Cyber Workforce Training Needs

CyberWatch is an Advanced Technological Education (ATE) Center, headquartered at Prince George's Community Colle**ge** and funded by a grant from the National Science Foundation (NSF). The CyberWatch mission is to increase the quantity and quality of the information assurance (that is, cybersecurity) workforce. The CyberWatch goals are focused on information assurance (IA) education at all levels, from elementary through graduate school, but especially the community college level, and include curriculum development, faculty professional development, student development, career pathways, and public awareness.

There is a perception that baccalaureate degrees are "minimum stakes" for hiring in the cybersecurity field. This perception is misinformed. The goal of the interactive session is to identify why these perceptions exist and engage in dialogue that will later assist CyberWatch in effectively changing these perceptions. CyberWatch seeks to raise awareness about the capabilities of community colleges in meeting the demand for a skilled cybersecurity workforce. In addition to describing the capabilities of Community Colleges in meeting workforce training needs, specific workforce training examples will be shared that have been delivered locally as well as nationally across both the public and private sectors. In addition, non-traditional approaches to sharing student capabilities with potential sponsors (for example participation in Collegiate Cyber Defense Competitions) will be described and linked to work force development aims. Participants will leave with the understanding of the ability of community colleges to deliver credit courses, non credit courses, and customizable contract training courses to meet workforce needs. In addition, participants will be actively engaged in dialogue focused on raising awareness about the resources available at community colleges (from awareness training to providing full curriculum) and capabilities of their students (from entry level employees to seasoned professionals).

Carrie Leary, Margaret Leary, and Costis Toregas, CyberWatch

Carrie Leary, Anne Arundel Community College/CyberWatch

Carrie Leary is a full-time Professor at Anne Arundel Community College in Arnold, Maryland, a NSA and DHS designated Center of Academic Excellence in Information Assurance 2-Year Education (CAE-2Y). In addition, she also serves at a Co-Principal Investigator of CyberWatch, a National Science Foundation (NSF) funded Advanced Technological Education (ATE) Center whose mission is to increase the quantity and quality of the information assurance workforce. Professor Leary previously served as the Director of Anne Arundel Community College's nationally recognized CyberCenter. Prior to entering academia, Ms. Leary served as an international consultant assisting organizations, from small businesses to Fortune 100 companies, to effectively use information technology and mitigate enterprise IT risk. She holds a B.S. in Business & Economics from Lehigh University and an MBA in Information Technology & International Business from American University. In addition, she has earned numerous Microsoft and CompTIA certifications as well as the designation as an EC-Council Certified Ethical Hacker.

Dr. Margaret Leary, CyberWatch

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. Costis Toregas, CyberWatch

Professor Toregas is the Assistant 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 Marketing Director and Industry Liaison for CyberWatch, 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. *(see pg 7 for full bio)*

Abstract: IT Competency Modeling: Linking the right people to the right training

Competency models serve as the foundation for determining curriculum requirements and associating specific training with positions within an organization. The Veterans Affairs (VA), Office of Information & Technology (OIT) developed and is currently implementing competency modeling for the GS-2210 IT job series.

The first role fully implemented at VA was the Information Security Officer (ISO). ISO's across VA are now using a validated competency model to semi-annually assess their proficiency level in key competencies and to select targeted training opportunities to fill skill gaps.

The competency models have allowed the ISO workforce to create tangible learning and development paths to follow for the duration of their careers. VA's IT Workforce Development group has teamed with VA's Learning University (VALU) and Plateau to implement a process utilizing Plateau's Talent Management System (TMS) for the delivery of competency modeling. TMS is a critical tool in implementing competencies and provides VA's ISO professionals with targeted training opportunities for professional development.

The presentation will explain the ISO competency model, describe how the competency model supports the ISO workforce, and to explain how the Talent Management System (TMS) aids in identifying and tracking competencies and associated learning events. Discuss the FISMA compliance reporting challenges for tracking role-base training and awareness training.

Terri Cinnamon, Veterans Affairs and Julie Wasielak, Booz Allen Hamilton

Terri Cinnamon, Director, IT Workforce Development Office of Information Technology, Veterans Affairs

Terri Cinnamon is the Director of Information Technology Workforce Development for the Office of Information and Technology at the Department of Veterans Affairs. A graduate from Wheeling Jesuit University, Terri joined the Department of Veterans Affairs in 1992. During her 19 years with VA, she has established a reputation within VA and across the federal community for leading innovative, practical, and effective information security training programs. Terri has been awarded the prestigious Government Information Security Leadership Award (GISLA), for "Distinguished service and commitment to excellence in implementing IT security programs" in 2006. She recently became a member of the Industry Advisory Council's (IAC) Partners Program, class of 2008. In March of 2011, Terri presented at the Federal Information Systems Security Educators' Association (FISSEA) Annual Conference and the Elliott's Masie Learning 2011 conference.

Julie Wasielak, IT Workforce Development Office of Information Technology, Booz Allen Hamilton

Julie Wasielak is an Associate for Booz Allen Hamilton and joined the firm in 2000. Ms. Wasielak has over 13 years experience as a system developer. She has extensive experience in Learning Management Systems, data analysis, application development and project management. Ms. Wasielak is the primary Talent Management System (TMS) representative to the Director of Information Technology Workforce Development for the Office of Information and Technology (OIT) at the Department of Veterans Affairs. In November 2011, Julie presented an overview of OIT competencies at the MASIE Learning conference.

	TRACK 1: Green Auditorium The New Era	TRACK 2: Lecture Room B Awareness, Training, and Education
4:15 – 4:40 pm	Smart Phone Security and Privacy: What Should We Teach our Users and How? – Dr. Norman Sadeh, Carnegie Mellon University/ Wombat Security Technologies, Inc.	Study Results: Failure-Triggered Training Trumps Traditional Training – Sean Palka and Avi Siegel, Booz Allen Hamilton

Abstract: Smart Phone Security and Privacy: What Should We Teach our Users and How?

Smart phones and tablets are rapidly establishing themselves as indispensable tools for a growing segment of the workforce. In the process, they are also forcing organizations to revisit many of their security policies and to confront difficult tradeoffs between productivity and security. Mobile devices also make it particularly easy and tempting for users to break across security boundaries. Our research shows that while users have been quick to adopt many of the new usage scenarios and applications that come along with these devices, their understanding of vulnerabilities associated with them remains rather limited.

In a first time, this presentation will review some of the main security vulnerabilities associated with poor end-user decisions and discuss the types of strategies and best practices one can realistically hope to teach everyday smart phone users One obvious challenge in this area is to determine how much users can effectively be expected to learn and to what extent security policies and technologies can realistically make up for those areas where training may be impractical or insufficient. A related challenge has to do with the diversity of devices, technologies and environments, the wide variety of usage scenarios mediated by smart phones today and the many vulnerabilities they entail.

The second part of this presentation will introduce a set of learning science principles and training tools we have developed to help train users to adopt safer smart phone practices. This will include a discussion of how we have prioritized learning objectives and designed training tools to focus on these objectives.

We will conclude with a discussion of lessons learned and recommendations for industry and government interested in improving their posture in this area.

Dr. Norman Sadeh, Professor (Carnegie Mellon University)/ Co-Founder & Chief Scientist (Wombat Security Technologies), School of Computer Science

Norman Sadeh is a Professor of Computer Science at Carnegie Mellon University, where he directs the Mobile Commerce Lab. His research interests span mobile and pervasive computing, Web Security and Privacy. He is also co-founder and co-director of the School of Computer Science's PhD program in Computation, Organizations and Society.

In the late nineties, Dr. Sadeh served as Chief Scientist of the $800M European Union's e-Commerce and e-Work research initiative, which at the time included all pan-European research in cyber security and online privacy. He's the author of "M-Commerce: Technologies, Services and Business Models", a best selling book published by Wiley in 2002. He's also co-founder, chairman and chief scientist of Wombat Security Technologies.

Dr. Sadeh received his PhD in Computer Science from Carnegie Mellon University and has authored around 200 scientific publications.

Abstract: Study Results: Failure-Triggered Training Trumps Traditional Training

Join us for a review of the results and lessons learned from a blind study on the effectiveness of Phishing Awareness Training. The study showed an approach employing sustained training and exercises can significantly improve learning transfer and on-the-job performance as opposed to traditional training approaches. The study included nearly 500 employees over nine months and analyzed multiple performance improvement approaches for e-mail phishing awareness and responses. One part of the study compared an interactive training session against a traditional static course (with content copied from a wiki). Imagine our surprise to find our targeted interactive training was no more effective than the static training content. In both cases, the majority of users passed the post-test with flying colors, but then more than 40% failed to react properly to an unannounced phishing attack when back on the job. Good thing there was another approach in the study that worked much better – failure-triggered training.

Sean Palka, Booz Allen Hamilton and Avi Siegel, Booz Allen Hamilton

Sean Palka, Lead Associate, Booz Allen Hamilton Sean Palka is a senior penetration tester with Booz Allen Hamilton. He has performed social engineering and penetration testing against networks and applications for a wide range of government and commercial clients, including several banks. He has created tools for executing complex phishing attacks and tracking of a wide range of response metrics. Sean recently won a "black badge" at DEFCON, the world's longest running and largest underground hacking conference, and is currently working on his doctoral dissertation in Computer Science at George Mason University.

Avi Siegel, Lead Associate, Booz Allen Hamilton Avi Siegel is a software development lead with Booz Allen Hamilton. He has been involved in the design and development of the STAR*Phish phishing awareness training capability, and additionally has experience in modeling & simulation, algorithm development, mobile applications, quantitative workforce analytics, application design, big data analytics, rapid prototyping, and robotics. He has worked primarily for government clients including the US Army and the Department of Veterans Affairs.

4:45 – 5:00 pm	Door Prize Drawing – Green Auditorium

Thursday, March 29, 2012 – *"New this year…Poster Session"*

8:00 – 8:45 am	Registration, Breakfast, and Networking
8:45 – 9:00 am	Morning Announcements Daily Announcers: Track 1: Louis Numkin Track 2: Rich Kurak, NASA
9:00 – 9:30 am	Keynote Address: Green Auditorium Digital Persona Protection Mark S. Loepker, Director, Office of the Secretary of Defense, Defense-wide IA Program (DIAP)

Keynote Abstract: Digital Persona Protection

What is a Digital Persona? And why are Members of the Federal Government, DoD, their Families and our Industrial Partners @ Risk?

Overview: Increasingly, members of US Government (USG) are facing threats from outside parties in the cyber realm due to their affiliation with USG. These threats pose risks to their digital persona. Think of your Persona as your digital footprint...every picture, text, email, blog, webpage about you to include purchases made by you online or off-line increases the size of your footprint plus it all begins @ birth. Your persona could be compared to a life-long medical history, from the second you are born, parents and family members start posting pictures, comments and information about you on the web and there will continue to be postings about you even after you have died, right? So every single data point from your past is on the web and is being collected somewhere, by someone for some reason-good or bad. The USG is leveraging the lessons learned from on-going and past events to develop an instruction assigning responsibilities and outlining procedures to be taken to mitigate and respond to threats to digital personas. Additionally, other guidance and best practices have been developed to assist those interested in both precautions against and responses to threats directed towards one's digital persona. Want to know more on how to protect you, your family and partners? Come sit, listen and learn ... We are here to Help!

Keynote Speaker: Mark S. Loepker, Director, Office of the Secretary of Defense, Defense-wide IA Program (DIAP)

Mark S. Loepker is the Director, Office of the Secretary of Defense, Defense-wide Information Assurance Program (DIAP). The DIAP's role is to ensure the DoD's vital information resources are secured and protected by unifying/integrating IA activities to achieve secure Net-Centric Global Information Grid (GiG) operations enablement and information superiority by applying a Defense in Depth methodology which integrates the capabilities of people, operations, and technology to establish a multi-layer, multi-dimension protection.

In past National Security Agency (NSA) assignments, Mark was the Committee on National Security Systems (CNSS), Secretariat Manager. The CNSS provides a forum for the discussion of policy issues, and is responsible for setting National Security Systems (NSS) national-level Information Assurance policies, directives, and instructions for U.S. Government (USG) departments and agencies. Mark was the Chief, NSA/CSS Pacific (NCPAC), Information Assurance (IA) Division where he was NSA's Senior IA Representative for the Pacific Theater. He led focused Pacific Command support in Information System

Security Engineering, network vulnerability evaluations, and operational force protection communications support. Mark was the Technical Director, NATO & CNSS, IAD Operations Group, Foreign Affairs Directorate (FAD) responsible for all foreign affairs technical matters affecting IA support to NATO and the CNSS. Mark led the genesis of *SECRET and Below Interoperability* (SABI) project; the Global Command and Control System (GCCS) Risk Assessment called TrueGRiTT; and the CNSS Certification & Accreditation Working Group publishing the first Federal level C&A process. Mark served for six years as the NATO INFOSEC Subcommittee National Co-Chairman and three years as the CNSS Subcommittee Co-Chairman.

Mark attended Purdue University receiving his commission through AFROTC in 1977. Lt Col (Ret.) Loepker began his military career at Whiteman AFB, MO serving as a Minuteman Missile Combat Crew Officer. He last served with the Command, Control, Communications and Computer Systems Directorate (ECJ6), United States European Command (USEUCOM), Stuttgart, Germany as Chief, Information Systems Security Division responsible for all European theater policy and policy enforcement concerning information warfare and communications and computer security. During his EUCOM tour, Lt Col (Ret) Loepker forward deployed in support of Operation Provide Comfort (Northern Iraq no fly zone) as the Director of Communications (C6). Prior to his USEUCOM assignment, Lt Col (Ret.) Loepker was the Assistant Director for Technical Services & Program Manager, Strategic Defense Initiative (SDI) MultiLevel Security (MLS) Systems Development. He directed the development and implementation of MLS systems supporting the SDI program and managed the development, installation and accreditation of the SDIO National Test Bed Network (NTBN). He served as a Defense Nuclear Agency (DNA) Program Manager responsible for the Supreme Headquarters Allied Powers Europe Nuclear Weapons Requirement Study, Allied Command Europe nuclear prelaunch survivability analytical methods and emerging nuclear detection technology in support of Special Operations Commander Europe.

Mr. Loepker retired from the Air Force and accepted his NSA position on 10 October 1999. He married Sandra S. Sandleben in 1978 and they have two children and two grandchildren.

	TRACK 1: Green Auditorium The New Era
9:30 – 10:00 am	IT Security Awareness – On a Budget - Joe Garrity, Library of Congress
10:00 – 10:15 am	Morning Networking Break

Abstract: IT Security Awareness on a Budget

Many IT Security shops in the Federal Government spend much of their energies preventing intrusion, identifying potential vulnerabilities, and securing their networks. As a result, most of the budget for the program is delegated to these areas. But one of the most important aspects of IT Security is often overlooked—Security Awareness. Annual training alone is not enough--giving users a sense of ownership in the security of their data is essential.

This short seminar focuses on how to develop an interesting awareness program on a budget. Innovative Security Awareness programs can be established with little to no money, and very little time. The presentation covers areas such as getting buy-in from management, bringing a sense of fun to awareness, creating websites and posters, guest speakers, contests and giveaways, etc. These simple methods can bring about change in attitude for users, and put your awareness program back on track.

Joe Garrity, Library of Congress

Joe Garrity is the IT Security trainer for the Library of Congress. In addition to all aspects of awareness training programs, he also 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 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.

	TRACK 1: Green Auditorium The New Era	TRACK 2: Lecture Room B Awareness, Training, and Education
10:15 – 11:05 am	**Game-Changing Technologies for Cybersecurity Awareness and Training –** Brenda Oldfield, Cypherpath LLC, Moderator; Panelists: Dr. Paulette Robinson, National Defense University/ iCollege; Dr. Daniel Laughlin, Morgan State University; Mr. Alex Cohen, Department of Energy	**Leveraging Human Factors for Effective Security Training –** Dr. Jason Hong, Carnegie Mellon University

Abstract: Game-Changing Technologies for Cybersecurity Awareness and Training Panel

Learners today use innovative technology to connect to all types of learning content.. Anytime, anywhere learning is where Cyber awareness should start. By providing a user driven relevant and engaging learning experience you can drive desired learning outcomes. This panel will explore how virtual worlds, social networking, crowd sourcing, gamification and advanced collaboration capabilities can provide new opportunities to motivate and engage learners at all levels.

This group of learning technologists will discuss current projects, programs, and research efforts to encourage the adoption and integration of 'game changing' technologies into your cybersecurity learning environments.

Brenda Oldfield, Moderator, Cypherpath LLC. Panelists: Dr. Paulette Robinson, National Defense University/iCollege; Dr. Daniel Laughlin, Morgan State University; Mr. Alex Cohen, Department of Energy

Moderator: Ms. Brenda Oldfield, Vice President, Cybersecurity Training and Education, Cypherpath LLC

Ms. Brenda Oldfield recently joined Cypherpath LLC, a cybersecurity training and education company that provides innovative workforce development solutions to government, academic and private sector organizations. Ms. Oldfield retired from Federal Government and her former position as Director of Cybersecurity Education and Workforce Development in the National Cyber Security Division of the U.S. Department of Homeland Security in 2011. She was previously the DHS Lead for the Cybersecurity Education component of the Comprehensive National Cyber Initiative (CNCI), which has since evolved into the National Initiative for Cybersecurity Education. And, Brenda was the FISSEA Educator of the Year recipient in 2009.

Panelists:

Dr. Paulette Robinson, Assistant Dean for Teaching, Learning & Technology, National Defense University/iCollege

Dr. Paulette Robinson is the Assistant Dean for Teaching and Learning for the Information Resources Management College (iCollege) at the National Defense University. She manages technology for the College and in this position, she manages a distributed learning instructional design group, reviews emerging technologies for inclusion in the innovations and simulations lab, implements technology and facilitates instructional use of technology for the College.

Dr. Robinson is also the leader for the Federal Consortium for Virtual Worlds, a group of over 1,000 from government (federal, state, local and international), industry, and academia who are interested in the use of virtual worlds in government, confronting and solving common issues, as well as sharing best practices.

Dr. Daniel Laughlin, NASA Learning Technologies - Goddard Earth Sciences, Technology and Research (GESTAR), Morgan State University

Dr. Daniel Laughlin is currently the NASA Learning Technologies (NLT) Project Manager at Goddard Space Flight Center. NLT supports the research and development of cutting-edge educational tools that combine NASA mission content with innovative technology and best teaching practices. NLT is primarily focused on the research and development of educational immersive synthetic environments and leads the games research effort for NASA's Education Office.
Dr. Laughlin received a Ph.D. in Education from American University with a focus on information technology in education and he did research in cognitive science experimenting with methods to explicitly teach critical and scientific thinking skills.

Mr. Alex Cohen, Technical Training Manager, Department of Energy

In his role of Technical Training Manager at the U.S. Department of Energy (DOE), Mr. Cohen is focused on the technical development of The National Training & Education Resource (NTER) project. At DOE, Alex serves in the Innovation, Technology & Performance Improvement Division of the Office of Human Capital where he works to support the agency's mission of Energy Independence and Strategic Security through technology implementation and process improvement. Formerly a project manager at the National Academies of Science and the Federation of American Scientists, Alex brings expertise in project management, software engineering, and research evaluation to the DOE team.

He has a B.S. in computer science and a minor in mathematics from the University of Massachusetts – Amherst and a Masters in Public Policy from George Mason University.

Abstract: Leveraging Human Factors for Effective Security Training

Usable security is an emerging field that lies at the intersection of human-computer interaction and computer security. Over the past few years, our group has been conducting research examining human factors in computer security, in particular looking at how to train people in a manner that is effective in practice.

One key element of our work has been to apply learning science principles, where learning science is a field that investigates how to help people learn content in a manner that is effective, can be retained, and can be transferred to other domains. Here, we will discuss some of our new approaches in computer security training, which has been field tested and published in peer-reviewed scientific publications.

Another element of our work has been to examining how to develop better user interfaces that can help people make better decisions. Here, we will discuss the results of user studies we have conducted looking at successes and failures in various interfaces. We will also discuss a model that presents a flow that describes how people see, understand, and are motivated to comply with security policies.

Dr. Jason Hong, Associate Professor, Carnegie Mellon University

Jason Hong is an associate professor in the Human Computer Interaction Institute, part of the School of Computer Science at Carnegie Mellon University. He works in the areas of ubiquitous computing and usable privacy and security. He is also an author of the book The Design of Sites, a popular book on web design using web design patterns. Jason is also a co-founder of Wombat Security Technologies, which focuses on the human side of computer security. Jason received his PhD from Berkeley and his undergraduate degrees from Georgia Institute of Technology. Jason is also an Alfred P. Sloan Research Fellow.

	TRACK 1: Green Auditorium The New Era	TRACK 2: Lecture Room B Awareness, Training, and Education
11:15 – 11:40 am	**Cybersecurity on a Budget -** Angela Orebaugh, Booz Allen Hamilton, Panel Chair; Robert E. Meyers, West Virginia University, J. Burton Browning and W. Cameron Kirby, Brunswick Community College	**Using Free Resources from OnGuardOnline.gov for Awareness, Safety, and Security –** Andy Hasty, Federal Trade Commission (FTC)

Abstract: Cybersecurity on a Budget

In today's climate of shrinking budgets, its important for educators to understand and implement free and low cost resources across People, Processes, and Technology to support enterprise level IT and security initiatives. This session will discuss free and low cost methods to perform cybersecurity awareness and training activities, teach fundamental cybersecurity practices, and identify and mitigate security vulnerabilities within your organization.

Angela Orebaugh, Booz Allen Hamilton, Panel Chair; Robert E. Meyers, West Virginia University; J. Burton Browning, Brunswick Community College; W. Cameron Kirby, Brunswick Community College

Angela Orebaugh, Booz Allen Hamilton

Angela Orebaugh is a cyber technologist, researcher, and executive with a focus in cybersecurity. She synergizes her 18 years of strategic and technical experience within commercial, academic, and government environments to advise clients on next generation technologies and disruptive innovation. Ms. Orebaugh is an internationally recognized author of several best selling technology books including, Wireshark and Ethereal Network Protocol Analyzer Toolkit and Nmap in the Enterprise. She is also an Adjunct Professor at George Mason University. Her current research interests include mobile device and application security, social media security, green technology, smart grid, continuous monitoring, and cyber physical systems. In 2011, Ms. Orebaugh was named Booz Allen Hamilton's first Cybersecurity Fellow.

Robert E. Meyers, West Virginia University

Robert E. Meyers has been a member of the West Virginia University Office of Information Technology since May 2004. Prior to his appointment as the Manager of Security Awareness for WVU Information Security Services in 2010, Bob served as the Assistant Director and Teacher Educator of the WVU Cisco Networking Academy Training Center. In this role he provided pedagogical and technical support to teachers and students in 6 countries and multiple states of the US. Bob's career includes work as an electronics service technician, a high school electronics instructor, a Federal Technology Challenge grant program coordinator, a teacher educator, and adjunct instructor at Kent State, Akron, Youngstown State, and West Virginia Universities teaching networking technologies and multiple classroom pedagogical and management courses. He is a graduate of Kent State University.

J. Burton Browning, Ed.D., Chair, Business, Engineering and Technology, Brunswick Community College

J. Burton Browning is Chair of Business, Engineering and Technology for Brunswick Community College, Supply, NC and national faculty member for Lesley University, Cambridge, MA. He regularly teaches graduate and undergraduate courses in many subjects, including: education, computer programming, computer security, networking, robotics, and systems design & analysis. His published works include refereed papers, books, chapters, and editor for texts on: computer programming, emerging technologies, and open source software. The latest books are on *Emerging Technologies* and *Design, Logic, and Programming with Python, a Hands-on Approach*. Receiving a doctoral degree in Technology Education from North Carolina State University in 1999, he has been working since the late 1980's in the technology field on many innovative projects, such as the North Carolina Information Highway, one of the New American Schools Development Corporation's grant sites "The Odyssey Project," robotics, innovative

education methods, and other technology-related initiatives. He lives in Eastern North Carolina, USA with his wife Anne and their six Siamese cats. He is available for training and consulting needs throughout the year.

W. Cameron Kirby, Brunswick Community College

An alumnus of the University of North Carolina Wilmington, William Cameron Kirby is currently a member of the Technology Department for the Brunswick County Public School System. This department is responsible for implementing and maintaining all IT infrastructure for the 19 schools across the rural county. In addition to this, he is also an adjunct instructor at Brunswick Community College where he teaches Unix/Linux to students in the Computer Programming curriculum. Areas of interest include: computer security, server virtualization, mobile technology, and open source solutions. Cameron Kirby currently resides In Southeastern NC and is available for training and consulting needs.

Abstract: Using Free Resources from OnGuardOnline.gov for Awareness, Safety, and Security

The Federal Trade Commission will demonstrate the free resources available through OnGuardOnline.gov, a dynamic website and blog that can be used for security awareness and education.

The FTC, in partnership with 15 other federal agencies, maintains OnGuardOnline.gov, a site to help people be safe, secure and responsible online. The site includes articles, videos, infographics, games and tutorials to teach home computer users, small businesses and employees about security-related topics like malware, phishing, P2P file sharing, Wi-Fi networks, mobile apps, and online tracking.

OnGuardOnline.gov – a partner in the Stop.Think.Connect. campaign and part of the National Initiative for Cybersecurity Education – features articles to help computer users be smart online, avoid scams, secure their computers, and protect kids online. The site also highlights resources for specific audiences, including teachers, parents, kids, military members, and IT professionals.

The site's videos, games and tutorials cover online safety and security topics like securing wireless networks, cyberbullying, malware, phishing and social networking. These multimedia resources are available for other agencies to use, embed, and share freely on their websites and blogs and in training and educational presentations.

The OnGuard Online Blog provides the latest cyber security news and practical tips from cyber security experts. The blog highlights important announcements about investigations, new education programs, research, and policy changes. Visitors can post questions for experts and sign up to get automatic updates when a new blog post is published. The FTC would like to encourage our federal partners and other federal agencies to write blog posts about their agency's cyber security activities.

The site also features the Net Cetera Community Outreach Toolkit. Regardless of one's experience as a speaker, this kit provides the resources and information needed to convey key points about protecting kids online. It includes a booklet for parents and teachers, a booklet for kids, videos for parents and kids, and a PowerPoint presentation. The kit and other printed resources featured on OnGuardOnline.gov can be ordered in bulk for free through the site.

Almost all of the free resources available at OnGuardOnline.gov are available in both English and Spanish. In fact, the site includes a toggle feature that allows site visitors to switch easily from one language to another.

OnGuardOnline.gov uses the ACSI customer satisfaction survey to measure how satisfied visitors to the site are. Since the re-launch of the site in September 2011, the site has maintained an average satisfaction score of 82, placing it amongst the highest ranked federal websites and well above the federal benchmark of 74.

The FTC would like to encourage other federal agencies to use the well-received free resources available at OnGuardOnline.gov to supplement their own cyber security awareness and education programs.

Andy Hasty, Mobile Technology Program Specialist, Federal Trade Commission

Andy Hasty is a Mobile Technology Program Specialist within the Federal Trade Commission's Bureau of Consumer Protection. Focused on the consumer protection implications of new and mobile technology, Andy helps manage OnGuardOnline.gov, the federal government's website to help computer users protect their personal information, secure their computers, and be on guard against Internet fraud. He holds a B.A. from the University of Virginia, and is currently pursuing his J.D. as an evening law student at The George Washington University Law School.

11:40 – 1:30 pm	**FISSEA Best Practice Session in Portrait Room (open 11:30 am - 4:00 pm)** **Lunch Break (NIST Cafeteria Rear opens at 12:10)** **NIST Tours – limited space; sign up at registration desk (first tour 11:40; second tour 12:30)**

FISSEA Best Practice Session

New this year…

This is an informal session for federal agencies (with support from contractors or vendors directly supporting that agency program) to share innovate projects, ideas, research, and programs with the FISSEA community. The session is Thursday, March 29, 11:30am-1:30pm (we will have the hall open until 4:00pm, but the primary time is between 11:30-1:30).

	TRACK 1: Green Auditorium The New Era	TRACK 2: Lecture Room B Awareness, Training, and Education
1:30 – 2:20 pm	**The National Institute for Cybersecurity Studies (NICS) Portal: A Cybersecurity Resource Tool for the Nation** - Peggy Maxson, Department of Homeland Security	**FedRAMP and Cloud Initiatives and How They Impact Security Awareness and Training** – Warren Udy, Department of Energy

Abstract: The National Institute for Cybersecurity Studies (NICS) Portal: A Cybersecurity Resource Tool for the Nation

Learn about this comprehensive online resource for information related to cybersecurity awareness and workforce issues – from staying safe and secure on line to the steps to prepare for and begin a career in cybersecurity, to increasing the cybersecurity workforce as developed by DHS and its partners, in support of the National Initiative for Cybersecurity Education (NICE). Currently in development, NICS–National Institute for Cybersecurity Studies–is a web-based portal that will provide information on cybersecurity workforce development, careers, education, awareness, and news and events. NICS is intended to be a tool for everyone–cybersecurity professionals, industry, academia, including students at the kindergarten through college levels, and the general public. The NICS portal will also include an interactive training catalog, which will provide a robust search capability, allowing users to search for training through such filters as location and career level. Join this session to hear about the process for mapping training to the specialty areas in the NICE framework and the tools available to you and your community through the portal for cybersecurity awareness, education and careers.

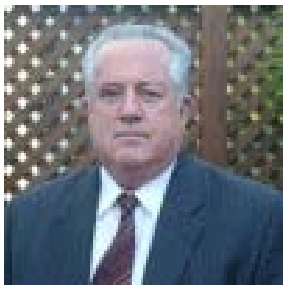
Peggy Maxson, Director, National Cybersecurity Education Strategy, Department of Homeland Security

On 19 April 2010, Ms. Maxson was appointed to her most recent position, 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-leading 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 34 years at the National Security Agency in managerial positions in operations, policy, foreign relations, customer service, and technology development.

Abstract: FedRAMP and Cloud Initiatives and How They Impact Security Awareness and Training

The expanding use of cloud services across the Federal Government is opening many new issues related to cybersecurity and privacy awareness for users and technical training for cybersecurity professionals. The Federal Risk and Authorization Management Program (FedRAMP) is a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. Beginning in summer 2012, Federal Agencies will be required to utilize FedRAMP security controls for all cloud services. The requirements for extended control sets for cloud applications and the concept of joint authorizations put forward by this program, however, can and should be extended to many applications, not just those in the cloud. In this presentation, Mr. Udy will introduce the concepts of the FedRAMP model and discuss how the approach will impact training and awareness programs across the Federal community.

Warren S. Udy, Department of Energy



Mr. Warren Udy is currently the Senior Cybersecurity Advisor to the Department of the Energy Chief Information Security Officer (CISO). As such he advises the CISO and represents the department on several interagency working groups dealing with cloud computing, new technologies and implementation of the agencies risk management framework. Prior to this assignment his duties included a detailed to GSA as the first Operations Manager for the Federal Risk and Authorization Management Program (FedRAMP) at for federal government-wide authorizations for the federal cloud computing initiative. His was the Director for the Office of Information Assurance and Cyber Security for the Energy Information Technology Services, responsible for the Department of Energy headquarters. He has over 30 years of leadership, program management, and technical management experience in operating and managing large, diversified organizations in Information Technology, Counterintelligence, and Cybersecurity environments. He spent 20 years in the U.S. Army as a Counterintelligence Officer, and successfully commanded/managed a large counterintelligence field office with resident offices that supported a major intelligence command. While in the U.S. Army he managed one of the first espionage investigations that included the removal of classified digital media. He was a Designated Approving Authority (DAA) for over seven years responsible for the nuclear testing programs at the Nevada Test Site. He was the federal manager for the NNSA Information Assurance Response Center; responsible for its initiation and initial growth. Since coming to Washington DC, he has worked as the Cybersecurity Program Manager for NNSA, the Office of the Under Secretary of Energy, and now within the Departmental OCIO. Mr. Udy holds the internationally recognized Certified Information Systems Security Professional (CISSP) from ISC2.

	TRACK 1: Green Auditorium The New Era	TRACK 2: Lecture Room B Awareness, Training, and Education
2:30 – 2:55 pm	**Workforce Management in a Continuous Monitoring Paradigm – How Our Organization Changed –** Jamie Noble, U.S. Census Bureau and Christian Neeley, Deloitte & Touche, LLP	**Interagency Solutions: Federal Cybersecurity Training Event (FedCTE)/Federal Virtual Training Environment (FedVTE) –** Benjamin Scribner, Department of Homeland Security (DHS)

Abstract: Workforce Management in a Continuous Monitoring Paradigm

While the concept of Information Security in the public sector has existed for decades, the specific requirements for its implementation continue to mature over time. As was the case with the introduction of FISMA in 2002, the impending transition to a Continuous Monitoring paradigm presents the federal government with a new set of challenges, both in creating the methodologies employed to secure its information systems as well as in developing the workforce upon whom it relies to design and deploy these new CM

programs. The security professional of the Certification and Accreditation era still has an important role in the CM programs of the future; however, it is incumbent on the industry to recognize the impacts to the workforce, prepare for staff retraining and design solutions that capitalize on the skills garnered over the last decade of federal IT security regulation.

Over the past two years, the US Census Bureau has been working to design and deploy a new Continuous Monitoring program that not only enables the organization through technology, but takes into account the human element in the overall strategy for program deployment and long-term sustainability. Through this process, the agency has come to understand the importance of the security workforce in the effective implementation of its strategic goals and the impact that programmatic design decisions can have on the workforce's ability to effectively execute their new tasks within CM.

In this presentation, we hope to share some of our lessons-learned as we led the Census Bureau through this transition to Continuous Monitoring. We will share how even moving a single responsibility from one person to another can end up driving efficiencies in the double digits, how properly aligning skill sets with job functions can create a more productive work environment, and how focusing on risk management at the executive level can lead to a more informed, engaged IT security workforce.

Jaime Noble, U.S. Census Bureau and Christian Neeley, Deloitte & Touche, LLP

Jaime Noble, C&A Program Manager, Office of Information Security, U.S. Census

Jaime Noble is the Certification & Accreditation (C&A) Program Manager for the Office of Information Security at the U.S. Census Bureau. She is charged with transitioning the Bureau's current C&A Program to the new Risk Management Framework through the implementation of a comprehensive continuous monitoring program promoting the concept of near-real-time risk management. Jaime graduated from The Pennsylvania State University in 2001 with a Bachelor's Degree in Management Science and Information Systems. She also has a Master's Certificate in IT Project Management from the George Washington University and earned her Certification and Accreditation Professional (CAP) certification in February 2010.

Christian Neeley, Senior Manager, Deloitte & Touche, LLP

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

Abstract: Interagency Solutions: Federal Cybersecurity Training Event (FedCTE)/Federal Virtual Training Environment (FedVTE)

We will provide an update to the Federal Virtual Training Environment (FedVTE) brief presented at FISSEA 2011. This free, online, and on-demand training platform is expected to begin accepting new users in 2012. In the first 15 minutes, we will explain what FedVTE is and how FISSEA participants can use the FedVTE to help close gaps in their department's or agency's specialized cybersecurity training. We will also provide a 25 minute demonstration of FedVTE's user interface, training delivery system, hands-on labs, and account management tools. The last 10 minutes will be reserved for questions from the audience.

Benjamin Scribner, Department of Homeland Security (DHS)

Mr. Scribner is the DHS lead for the government-wide implementation of the Federal Virtual Training Environment and the Federal Cybersecurity Training Exercise Program. He previously served in the DoD CIO office supporting implementation of the DoD 8570 Information Assurance Workforce Program. Mr. Scribner holds two Master's degrees in Information Management and Business Administration from George Washington University in Saint Louis.

	TRACK 1: Green Auditorium The New Era
3:05 – 3:30 pm	**Education is Key to Understanding Cyberbullying and the Dangers of Social Networking Sites** – Dr. Karen Paullet, Edvancement Solutions
3:30 – 3:40 pm	**Door Prize Drawing and Conference Close**

Abstract: Education is Key to Understanding Cyberbullying and the Dangers of Social Network Sites

In order to fully understand cyberbullying and the risks associated with social network sites it is critical that adults understand the consequences that can occur from inappropriate communication taking place in the digital world. The laws and problems associated with the digital world will be discussed in detail. Adults must keep an open line of communication with children so that if a problem occurs they will be willing to talk about problems that take place in the cyberworld. Parents and educators must keep their kids informed about the inappropriate behaviors associated with the use of technology. One of the biggest challenges facing law enforcement is the anonymity. Often times it can be difficult to figure out who is actually sending the threats. There are many ways to disguise ones identity through the use of electronic communication. It is imperative that parents, teachers and law enforcement work together to solve this growing problem. Topics to be discussed include cyberbullying, sexting, predators, the dangers associated with social networking and the laws surrounding these issues.

Karen Paullet, Edvancement Solutions

Dr. Karen Paullet is the Cyber Security Academy Chair with Edvancement Solutions promoting security awareness to educators, administrators and students grades 3-12. She teaches at Robert Morris University and American Public University in their Cyber Security Programs. 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.

3:30 – 3:40 pm	**Door Prizes Drawing and Conference Close**

- Conference Director: Patricia Toth, NIST
- Conference Coordinator: Peggy Himes, NIST
- Masters of Ceremonies: Cheryl Seaman, Gretchen Morris, Lance Kelson, Richard Kurak, and Louis Numkin (still coming back out of retirement for us)
- All the speakers and panelists for donating their energy, time and knowledge
- 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 contests. Special thanks to the judges.
- Participants for sharing their ideas and programs in the first FISSEA Sharing Best Practices Session and to Susan Hansche for coordinating this event.
- Graphic Artist, Reggie Leger, Avaya Government Solutions for designing the cover. Can you identify what the icons represent through the years?
- Conference Assistance: (integral to this effort) Susan Hansche, Gretchen Morris, Angela Orebaugh, Sue Farrand, and Al Lewis
- FISSEA 2012 Technical Working Group Members for their contributions throughout this past year and serving as the Program Committee: Daniel Benjamin, Art Chantker, Terri Cinnamon, Susan Farrand, Susan Hansche, Peggy Himes, John Ippolito, Chris Kelsall, Lance Kelson, Richard Kurak, Albert Lewis, Gretchen Morris, Cheryl Seaman, Patricia Toth, Mark Wilson, Marirose Ziebarth.
- NIST Supporters: NIST Computer Security Division, Kevin Stine. NIST Conference Office: Mary Lou Norris and Teresa Vicente. NIST AV technicians.
- Attendee and speaker gifts purchased from Julia Gagnon, PMSI – Professional Marketing Services
- Registration Coordination and Vendor Support: Federal Business Council (FBC): Shannon Grady

- Prize Drawing Gift Contributors:
  - SANS Institute, Brian Correia - 3 IPADS
  - Federal IT Security Institute (FITSI), Maribeth Kuzmicki – a Kindle Fire
  - Potomac Forum, Art Chantker - FISSEA conference ad in Gov Exec, book by Mel Greer: *"Software as a Service Inflection Point, Using Cloud Computing to Achieve Business Agility"*, Potomac Forum Executive Coaster Sets, Travel Security Kits (TSA and PC Combination Locks)
  - LunarLine, Melissa Dawson – A CLASSPASS training voucher for a free IA Cybersecurity class at their facility
  - The Hacker Academy, Aaron Cohen – a free 1 year license to The Hacker Academy online training course

- ISC2, Steve Chichester - CISSP CBK Study Guide
- Cengage Learning – books:
  - *"Official Certified Ethical Hacker Review Guide: For Version 7.1, 1st Edition"* by Steven Defino and Larry Greenblat;
  - *"Cybersecurity: The Essential Body of Knowledge"* by Dan Shoemaker and Wm. Arthur Conklin;
  - *"Roadmap to Information Security: For IT and Infosec Managers, 1st Edition*", by Michael Whitman and Herbert Mattford
- Sue Farrand - Symantec backpack & book, *"Worm: The First Digital World War"* by Mark Bowden
- Defense Cyber Investigations Training Academy (DCITA), Dr. Loyce Best Pailen – Miscellaneous DCITA motivational giveaways
- Food and Drug Administration, Sara Fitzgerald and Mo Moore – motivational items (Security Awareness six pack with various flavors and security tips)
- Rebecca Herold & Associates, LLC – book *"Managing an Information Security and Privacy Awareness and Training Program"* by Rebecca Herold
- CompTIA, Carol Balkcom, Tara Dean, Joe Padin – 2 CompTIA/Wiley exam and courseware bundles
- Patricia Toth - NIST fleece jacket

Attendees for expressing their continued confidence in FISSEA's ability to provide cost effective training by their conference attendance.