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

Bridging to the Future – Emerging Trends in Cybersecurity

Bios/Abstracts

Conference presentations will be posted to the FISSEA website, www.fissea.org

Tuesday, March 15, 2011

8:00 – 8:45 am	Registration, Breakfast, and Networking
8:45 – 9:00 am	FISSEA Welcome: Mark Wilson, NIST, FISSEA Conference Director NIST Welcome: Jim St. Pierre, Information Technology Lab, NIST Daily Announcers: Gretchen Morris (Track 1) and Al Lewis (Track 2)
9:00 – 9:45 am	Keynote Address: Green Auditorium Overview of the National Initiative for Cybersecurity Education (NICE) Dr. Ernest McDuffie, NIST
9:45 – 10:00 am	Morning Networking Break
10:00 – 11:45 am	NICE Panel Timothy Fraser, DHS, National Protection and Programs Directorate – Track 1 Michael Lach, U.S. Department of Education – Track 2 Maureen B. Higgins, OPM and Jacqueline Caldwell, OPM – Track 3 Peggy Maxson, DHS - Track 4

Keynote: Dr. Ernest McDuffie, 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.

Abstract: Overview of the National Initiative for Cybersecurity Education (NICE)

Dr. McDuffie will present a high level overview of the National Initiative for Cybersecurity Education (NICE) and provide an update of its most current activities.

Timothy Fraser, Director National Cybersecurity Awareness Campaign, Department of Homeland Security, National Protection and Programs Directorate

Timothy Fraser is the Director of "Stop. Think. Connect." – a national cybersecurity awareness campaign led by the Department of Homeland Security and a key element of President Obama's 2009 Cyberspace Policy Review. Stop. Think. Connect. seeks to enhance the public's understanding of cyber threats and engage individual citizens to develop safer cyber habits that will help make them and their networks more secure.

Prior to the cybersecurity awareness campaign, Fraser served as Director for Public Engagement in the Office of the Federal Coordinator for Gulf Coast Rebuilding, where he focused on establishing relationships and partnering with non-profit organizations, private business, and local and state officials in the Gulf Coast region.

Prior to government service, Fraser led the Get Out The Vote (GOTV) efforts for he "Obama for America" presidential campaign in Indiana and worked on numerous political campaigns dating back to 2002. Fraser brings to DHS experience in civic engagement, community organizing, grassroots campaigns, and inter-agency communications.

Abstract: Track 1

Stop. Think. Connect. is a national public awareness effort to guide the nation to a higher level of Internet safety by challenging the American public to be more vigilant about practicing good "cyber hygiene." It will persuade Americans to see Internet safety as a shared responsibility—at home, in the workplace, and in our communities—and demonstrate that shared responsibility by bringing together a coalition of federal, state and local government, as well as private sector partners.

The creation of Stop. Think. Connect. was the result of an intensive collaborative effort over the past year from the Online Consumer Security and Safety Messaging Convention, an effort organized by the National Cyber Security Alliance (NCSA), the Anti-Phishing Working Group (APWG), key industry leaders, government agencies, and nonprofits.

Led by the Department of Homeland Security, the ultimate goal of Stop. Think. Connect. is to raise awareness among the American public about the need to strengthen cybersecurity—and to generate and communicate new approaches and strategies to help Americans increase their safety and security online.

The Stop. Think. Connect. Campaign kicked off on October 4, 2010, in conjunction with National Cyber Security Awareness Month.

Michael Lach, Special Assistant for Science, Technology, Engineering, and Mathematics Education, U.S. Department of Education

Michael Lach leads science, mathematics, engineering, and technology education efforts at the U. S. Department of Education. Previously, Michael was Officer of Teaching and Learning for the Chicago Public Schools, overseeing curriculum and instruction in the 600+ schools that comprise the nation's third largest school district. Mr. Lach began his professional career teaching high school biology and general science at Alceé Fortier Senior High School in New Orleans in 1990 as a charter member of Teach For America, the national teacher corps. After 3 years in Louisiana, he joined the national office of Teach For America as Director of Program Design, developing a portfolio based alternative-certification system that was adopted by several states. Returning to the science classroom in 1994 in New York City Public Schools, and then back to Chicago in 1995 to Lake View High School, he was named one of Radio Shack's Top 100 Technology Teachers, earned National Board Certification, and was named Illinois Physics Teacher of the Year. He has served as an Albert Einstein Distinguished Educator Fellow, advising Congressman Vernon Ehlers (R-MI) on science, technology and education issues. He was lead curriculum developer for the Investigations in Environmental Science curriculum developed at the Center for Learning Technologies in Urban Schools at Northwestern University and published by It's About Time, Inc. As an administrator with the Chicago Public Schools, he led the district's instructional improvement efforts in science and mathematics in a variety of roles between 2003 and 2007. He earned a bachelor's degree in physics from Carleton College, and master's degrees from Columbia University and Northeastern Illinois University.

Abstract: Track 2

Michael Lach will speak about recent efforts to improve formal cybersecurity education, including the connection between cybersecurity education and STEM education more broadly. He will also discuss the administration's efforts to improve STEM education, including the NICE formal cybersecurity education strategy.

Maureen B. Higgins, Assistant Director, Agency Support and Technical Assistance, Office of Personnel Management (OPM)

As the Assistant Director for Agency Support and Technical Assistance at the Office of Personnel Management (OPM), Ms. Higgins is responsible for working with Federal agencies to promote efficient and effective human capital management and to implement key human resources initiatives and priorities. Ms. Higgins is also currently leading OPM's work on the National Initiative for Cybersecurity Education.

Ms. Higgins has over twenty years experience in the Federal government. She previously served as the Deputy Associate Director, Center for Workforce Information and System Requirements at OPM, and she has held a variety of positions with the Department of Defense, Air Force and Joint Chiefs of Staff including two assignments in Europe. She has extensive experience in civilian and military human resources management and policy development, management of personnel information systems and transformation projects, and programming, budgeting and resource management.

Her education includes a Master of Strategic Studies from Air War College, a Master of Public Administration from Troy University, a Bachelor of Arts in Urban Affairs from Virginia Tech, and completion of the Federal Executive Institute's Leadership for a Democratic Society.

Dr. Jacqueline Caldwell, Personnel Research Psychologist, Office of Personnel Management (OPM)

As a Personnel Research Psychology in the Classification and Assessment Policy Group at the Office of Personnel Management (OPM), Dr. Caldwell is responsible for conducting research and providing technical assistance in various areas of human resources management. She is the Project Manager for the Cybersecurity Competency Model Study. Dr. Caldwell has over twenty-five years' experience in the Federal government.

Her education includes a Ph.D. in Psychology from Ohio State University, a Bachelor of Arts in Psychology from the University of Iowa.

Abstract: Track 3

The Cyberspace Policy Review (May 2009) recognized the need to "Develop a strategy to expand and train the workforce, including attracting and retaining cybersecurity expertise in the Federal government." The Office of Personnel Management (OPM) plays a key role in the National Initiative for Cybersecurity Education (NICE) by leading the Federal Workforce Structure efforts. Over the past year, OPM has been working with Federal agencies to understand and define cybersecurity work in the Federal government and to identify and analyze barriers, challenges and successful recruiting practices. OPM analyzed information collected via a workforce survey to identify the tasks and competencies that are most important for successful performance in Federal cybersecurity positions. Competency models were published February 16, 2011 and will be used to inform Federal human resources policy and to assist employees in career development and training, as well as to help organizations with workforce planning, selection, and performance management. The presentation will discuss these and other key steps towards ensuring Federal agencies can attract, recruit and retain skilled employees to accomplish cybersecurity missions.

Margaret (Peggy) Maxson, DHS - Track 4

On 19April 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 as the Education Portfolio Manager on the Director of National Intelligence Joint Interagency Cyber Task Force (JIACTF). At the JIACTF, she led a cybersecurity education subgroup of the White House Information and Communication Infrastructure Interagency Policy Committee (ICI-IPC), which resulted in the accepted recommendation and subsequent implementation of the establishment of NICE.

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 Bridging to the Future – Emerging Trends in Cybersecurity	
11:45 – 12:15 am	Business Meeting: The Future of FISSEA Mark Wilson, FISSEA Board Chair and Matthew Scholl, NIST	
12:15 – 1:15 pm	Lunch Provided – NIST Cafeteria Rear	
1:15 – 1:45 pm	Presentation of FISSEA Security Contest Winners: By Gretchen Morris, DB Consulting/NASA Presentation of 2010 FISSEA Educator of the Year: By Brenda Oldfield, DHS, FISSEA Educator of the Year 2009 Door Prize Drawing	
	TRACK 1: Green Auditorium Bridging to the Future – Emerging Trends in Cybersecurity	TRACK 2: Lecture Room B Open Forum
2:00 – 2:25 pm	The 6 Skills of Highly Effective & Validated InfoSec Professionals Sondra Schneider, Security University	ISS LOB Security Awareness Training Tiers 1 and 2 Panel Timothy McBride, Department of Homeland Security, Moderator. Panel Members: George Bieber, DoD; John Feldmann, DoS; Terri Cinnamon, VA; Dave Zwach, DoS; Gretchen Morris, DB Consulting/NASA; William Peratino, OPM
2:35 – 3:00 pm	IT Security Awareness on a Budget Joe Garrity, Library of Congress	
3:00 – 3:15 pm	Afternoon Networking Break	

Sondra Schneider, Security University

Sondra J. Schneider's contributions to information assurance, computer security and professional education could well be summed up as globally illuminating risk preparedness through building bridges. In 12 years as CEO of Security University she has sought to bring a consistent methodology of enhancing the technical skills required to safeguard business, military and government information. Her training curriculum has been singularly recognized in meeting the needs of US financial markets, the US Intelligence community, manufacturing, medical and global industries where she has worked on bridging courses, programs, departments, and professions through the promotion of information security and assurance.

Sondra has been an education leader promoting actual threat recognition of data risks/vulnerabilities; from business awareness to hands-on remediation. She exhibits the kind of drive, ethics and professionalism that one strives to identify when looking for these critical business services. To find such consistent excellence over a span of time in an environment that has seen such a dynamic change in data security and assurance is truly admirable.

In early 2000, Sondra focused her company to change how agencies provided risk mitigation skills, forever changing the standard education curriculum by requiring students to actually know how to secure infrastructures. She structured Security University's education program from the ground up to deploy sound multi-tier/defense-in-depth solutions, while also incorporating the identifying, combating and remediation of malicious activities. Her ongoing efforts also saw the realization that no one program or certification adequately prepared an individual for truly becoming an information security profession. Security University has been industry recognized by the Center for Academic Excellence as the only non-academic education company to achieve 4011,4102,4013,4105,4016E,I,A CNSS approval and has recently been selected to be approved to the 8570 Certification List with 5 performance based security certifications.

Sondra has consistently led the security education industry with her foresight on what skills are currently needed; always looking to the future. This focus is evidenced with Security University having trained over 24,000 individuals globally providing the foundation for over 2,500 security professionals completing their Q/ISP classes and Certifications, and numerous individuals achieving the only performance based "validated: Qualified/ Information Security Professional Certificate. Additionally over 2,500 professionals have taken their CWNA, CWSP and QWAD certifications from Security University who recognized in 2003 that wireless infrastructure required tactical hands-on remediation and set out to provide leadership in wireless education. Besides engaging with her peers, she consistently reaches out to industry thought leaders to hear what they are recognizing as evolving issues. Her ability to listen and translate these engagements into meaningful course offerings has consistently made her Security University one of first choice, an easy recommendation and a value added proposition.

Abstract: The 6 Skills of Highly Effective & Validated InfoSec Professionals

The Basic Principles of InfoSecurity are Universal and Timeless principles of processes and methodology. Since values govern people's behavior and principles ultimately determine the consequences, it's critical that the security process and methodology used to educate and train our Cyber security professionals ensures the security work force is not just certifying but qualifying our InfoSec Professionals. The presentation review's and discusses the 6 Skills of Highly Effective & Validated InfoSec Professionals and the

steps necessary to achieve that goal. The 6 skills are presented in a series of infosecurity skills certifications, manifesting as a progression from certified via validated via qualified.

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.

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.

ISS LOB Security Training Tier 1 and Tier 2 Panelists

Panel Moderator: Timothy McBride, Department of Homeland Security Panel Members: George Bieber (DoD): Tier I SSC/Tier II SSP; John Feldmann (DoS): Tier I SSC; William (Bill) Peratino (OPM); Terri Cinnamon (VA): Tier II SSP; Dave Zwach (DoS): Tier II SSP; Gretchen Morris (DB Consulting/NASA): Tier II Shared SSP

Timothy McBride, Acting Program Manager
U.S. Department of Homeland Security, Office of Cybersecurity and Communications, National Cyber Security Division (NCSD), Federal Network Security, Requirements and Acquisition Support

Mr. McBride has 15 years of experience managing, developing, and deploying information technology and security solutions in the Federal and Commercial environments. Currently Mr. McBride is assigned to the Department of Homeland Security's, Requirements and Acquisition Services Program in the National Cyber Security Division's Federal Network Security Branch. Mr. McBride holds a BA from the University of Hawaii, an MS from The George Washington University and is a Certified Project Management Professional (PMP). Mr. McBride is a Co-Chair on the Continuous Monitoring and Risk Scoring Working Group.

George Bieber, Director, IA Workforce Improvement Program Defense-wide Information Assurance Program (DIAP), Department of Defense

Mr. George Bieber is Director, IA Workforce Improvement Program, Defense-wide Information Assurance Program (DIAP). In this capacity he has oversight responsibility for all aspects of the Department's IA and cybersecurity education, training, and awareness activities, the DoD IA Scholarship Program, and workforce management issues.

Previously he was Chief, Information Assurance (IA) Education, Training, Awareness (ETA) and Products Branch, Defense Information Systems Agency. He managed the development, production and dissemination of Department of Defense (DOD) IA training and awareness materials.

John Feldmann, JSAS Business Manager, U.S. Department of State

John Feldmann was appointed as the Division Chief of the Policy, Liaison, and Reporting Division on February 1, 2010, and he serves as the Business Manager for the ISSLOB Cybersecuity Awareness SSC. He has served the Department in various assignments over

the years that includes Division Chief of Systems Integrity and as the Administrative Officer at the Diplomatic Telecommunications System Program Office (DTS-PO). John earned his undergraduate degree from the University of Maryland. He received his graduate degree from the University of Southern California. He also maintains his CISSP and CISM certifications.

Terri Cinnamon, Director of Information Technology Workforce Development, Department of 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. Terri has 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 Learning Management System (LMS). Terri and her team 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.

Gretchen Morris, CISSP, Consultant, DB Consulting Group supporting NASA ITSATC

Mrs. Gretchen Morris has been developing on-line course content as a major part of her work over the past 10 years. She also has been part of the governance and administration of the LMS that houses the content. Training difficult concepts is her favorite thing to do. She has fifteen years teaching and troubleshooting experience on a variety of software packages and hardware configurations. She has a solid and diverse background in computer software/hardware, electronics troubleshooting, training, course development, and management. She has a Bachelor of Applied Science in Resource Management degree from Troy State University, and a Master of Arts degree in Biblical Counseling from Trinity Theological Seminary. She is a CISSP and earned the Master Training Specialist designation while serving as a Navy Instructor. In her current position with DB Consulting Group as a Consultant, she is a vital part of the NASA IT Security Awareness and Training Center team, which supports over 55,000 users across the Agency.

William (Will) Peratino, Director of Innovation, Office of Personnel Management/Emerging Solutions Program Office

Mr. Peratino has close to 40 years service with the federal government across all facets of human performance improvement. He is currently the Director of Innovation within OPM's Emerging Human Resource Solutions group employing advanced technology solutions to a range of training, performance support, testing, and human capital challenges. Previously as the Director of the E-ov initiative GoLearn, the federal government's on-line university, Mr. Peratino oversaw development and delivery of on-line training and LMS implementations for all cabinet-level and multiple small agencies.

Prior to joining OPM, Mr. Peratino worked in the US Department of Labor, Assistant Secretary for Policy Office in the capacity of Director of Distance Learning Policy and Programs using technology-based solutions to enhance the performance and productivity of individuals. Serving as the Director of New and Emerging Technologies, US Department of Labor Office of Assistant Secretary for Policy he employed open-source software to develop a government-owned web publishing and on-line knowledge management repository: Workforce Connections which he made freely available as an Open Source "Custom Distribution" and was downloaded by thousands of organizations worldwide to support their training development. While at Labor, Mr. Peratino also served as Deputy Director of the Federal Advanced Distributed Learning Co-Laboratory in Alexandria, VA as a key liaison between government and the commercial sector to lead technical efforts, which promote the portability and interoperability of systems and applications government and industry-wide via the SCORM specification.

Through the fall of 2000 Mr. Peratino was the Director of Distance Learning Programs at the Defense Acquisition University where he designed, developed, and implemented the first virtual university in all of government. Mr. Peratino as the Director of Distance Learning Programs, managed the redesign and modernization efforts of more than 70 distributed learning courses for the Defense Acquisition University. In addition, Mr. Peratino chaired the Content Advocacy Group of the Advanced Distributed Learning Initiative (ADLNET.ORG). This initiative, sponsored by the Office of the Secretary of Defense and the White House Office of Science and Technology Policy is evaluating ways to use technology to support life-long learning.

Prior to joining DAU in 1994 Mr. Peratino, while at the Bureau of Medicine and Surgery, U.S. Navy, managed the design, development, and delivery of the Computer Assisted Medical Interactive-video System (CAMIS) which was the largest government multimedia education and training initiative at that time. CAMIS represented thousands of hours of multimedia-based medical training developed specifically for Naval Independent Duty Corpsman/Emergency Medical Technicians, nurses, and physicians worldwide.

With this wealth of experience on through the evolution of training and the ongoing challenges, Mr. Peratino will illustrate some of the past, present and future challenges facing the human performance improvement industry.

Dave Zwach, Chief, Information Assurance Branch, U.S. Department of State, Diplomatic Security Training Center

David Zwach is Security Engineering Officer and Chief of the Information Assurance Branch (DS/SECD/IAB) at the Diplomatic Security Training Center. He oversees the Departments Information Assurance and Cybersecurity training programs. IAB provides Tier 2, role-based training to more than 1000 USG employees worldwide each year. IAB is an Information Systems Security Line of Business (ISS LOB) Shared Service Provider (SSP).David obtained a Bachelors of Mechanical Engineering degree from the University Minnesota Institute of Technology (MNIT) in 1985. In 1996, David obtained a Masters in Business Administration (MBA) degree from George Washington University. In 1987, Mr. Zwach joined the Department of State as a Security Engineering Officer and he was appointed as a career member of the Foreign Service in 1989.Mr. Zwach served the Department's Counter Measures Program until 1992. He then served at the US Embassy in New Delhi from 92-94. He served in excursion assignments as an Environment, Science and Technology Officer and as Political Military Affairs Officer from 1995-99. Mr. Zwach served in the Engineering Services Center at US Consulate General Frankfurt Germany from 1999 to 2001, providing technical support to US missions in Europe. In 2001, he created the Quality and Liaison Branch under the Bureau of Diplomatic Security which is responsible for inspecting technical security installations at US Embassies and Consulates. Mr. Zwach managed Diplomatic Security's Field Support Branch from 2004-06. Mr. Zwach served as Officer In Charge (OIC) of the Engineering Services Center at the US Embassy in Abu Dhabi, United Arab Emirates from 2006-2009. He was responsible for technical security services to 16 US Missions in the Arabian Gulf region.

Abstract: ISS LOB Security Training Tier 1 and Tier 2 Panel

The Information Systems Security Line of Business (ISSLOB), under OMB mandate, provides cost savings / avoidance through the utilization of shared services. Tim McBride will lead the discussion on how Shared Service Centers (SSCs) provide effective Training options that fulfill required standards / mandates at little to no cost to the federal community. Participants can expect to hear from a panel of SSC Providers on their offerings for both general and role-based training, as well as receive an overview of the upcoming Continuous Monitoring portion due out this year.

Mr. Peratino will demonstrate the following: NIST Mandated IT Role-Based Security Training Available for Network Administrators. OPM Office of Emerging Solutions announces the availability of the first in a series of new immersive environment, avatar-based IT Security courses. The first course is designed for Network Administrators to fulfill the NIST mandatory agency training requirements.

	TRACK 1: Green Auditorium Bridging to the Future – Emerging Trends in Cybersecurity	TRACK 2: Lecture Room B Open Forum
3:15 – 4:05 pm	Hacking Techniques for Hacking Stuff Rob Murphy, ISI Professional Services	Securing The Human Marcus Sachs, Verizon

Rob Murphy, Senior Vice President, IT Services Group, ISI Professional Services

Rob Murphy transitioned from the United States Marine Corps and joined the team at ISI Professional Services as the Senior Vice President of IT Services Group. He holds a Masters in Information Technology Management from the Naval Postgraduate School in Monterey, CA and maintains the professional certifications of CISSP, CEH, CHFI, Network+ and Security+. He is an Adjunct Professor for The College of Southern Maryland, University Maryland University College and has spoken at a variety of security conferences to include Defcon, DoD Cyber Crime Conference, USMC IA Conference, the NSA Red Team/Blue Team Symposium, MITRE IPv6 Symposium, Redstone Arsenal IA Conference and TechNet Mid-America. His areas of expertise include network security, information security and wireless network security and administration. Rob has developed several tools throughout the years to include MACSpoof and an IPv6 covert channel tool called v2net. Finally, Rob is the author and designer of Warlock Games (warl0ck gam3z) which is an online Jeopardy style architecture capable of hosting a variety of challenges and has been showcased both in the academic realm as well as conferences for participation and competition.

Abstract: Hacking Techniques for Hacking Stuff

Ready to learn hacking techniques? Start off with attack vectors hackers use in the cyber world to locate potential targets. Dissect SQL injection and witness how hackers can take over a website. Move into the world of poorly configured systems that allow Internet access into a domain with administrative-level privilege. Need extra storage for that questionable software? Want to know how your

credit card number was stolen? Ever wondered if your online bank was safe to log into? Do you really have to pay for wireless Internet access? Does anybody still use WEP? You use the TOR network so you must be safe, right? How secure is SSL? How does SPAM get into the military network? Tired of hearing about specially crafted packets, turning off unused services and making sure your patches are up to date? This is a straightforward, no holds-barred presentation on how "stuff" gets hacked. Feel free to bring pencil and paper, but take notes at your own risk.

Marcus Sachs, Vice President, National Security Policy, Verizon

Marcus Sachs serves as vice president of government affairs for national security policy at Verizon in Washington, DC. Prior to joining Verizon in August 2007, he was the deputy director of SRI International's Computer Science Laboratory. Marcus served as the director of the SANS Internet Storm Center from 2003 to 2010 and is an internationally recognized computer security expert. He brings nearly 30 years of professional experience to SANS, including 20 years of active military service as an officer in the United States Army and two years of national cyberspace security policy development as a Presidential appointee to the National Security Council staff in the George W. Bush administration. Marcus was the first cyber security official assigned to the Department of Homeland Security in 2003 where he developed the initial concept and strategy for the creation of the United States Computer Emergency Readiness Team. He was also a founding member of the Defense Department's Joint Task Force for Computer Network Defense, created in 1998 as the first US military organization designed to fight foreign threats in cyberspace. He is currently the secretary of the Communications Sector Coordinating Council and is a member of the CSIS Commission on Cyber Security for the 44th Presidency. Marcus is a licensed professional engineer in Virginia.

Abstract: Securing The Human

Organizations have traditionally invested most of their security in technology, with little effort in protecting their employees. As a result, many attackers today target the weakest link, the human. Awareness, not just technology, has become key to reducing risk and remaining compliant. This high-level talk designed for management explains why humans are so vulnerable, how they are being actively exploited and what organizations can do about it.

Key points include:

- How humans are nothing more than another type of operating system, albeit a highly vulnerable one.
- Why humans are so bad at judging risk and how attackers exploit these vulnerabilities.
- How an effective awareness program patches these vulnerabilities and reduces risk.
- How to develop a modular and flexible program that reach multi-cultures.
- How to create and effectively use metrics.

	TRACK 1: Green Auditorium Bridging to the Future – Emerging Trends in Cybersecurity	TRACK 2: Lecture Room B Open Forum
4:15 – 4:40 pm	Personally Identifiable Information: An Interactive Story Carolyn Schmidt, DOC	Social Insecurity: Social Media Challenges for Cyber Security Professionals Albert Lewis, HP Enterprise Services
5:30 pm	Dinner Get Together – Location TBD (sign up at conference; not included in registration fee)	

Carolyn M. Schmidt, Senior Program Manager, Office of the Chief Information Officer, U.S. Department of Commerce

Ms. Schmidt is a senior Program Manager for Information Technology (IT) Security Training and Education for DOC. In this role, she is responsible for establishing an IT security training plan for DOC's staff who have significant information security responsibilities. In 2006, Ms. Schmidt was awarded the U.S. Department of Commerce Bronze Medal in this subject area, and in June 2008, and graduated from the Commerce Science & Technology Fellowship Program in June 2008.

Prior to assuming her current assignment, Ms. Schmidt's experience has encompassed digital library research, systems administration, web development and design, development of agency and Department-wide IT security policy, implementation of agency level policy and procedures, and certification and accreditation activities of information systems. She has spoken at several conferences in support of her work in research and in IT security.

Abstract: Personally Identifiable Information: An Interactive Story

The course is designed to bring awareness about Personally Identifiable Information (PII), and is presented through a day long story in which various PII mishaps occur. The training scenarios incorporate various teaching points, addressing each individually through exploratory decision-making and/or mini-games essential to the student's progression through the game, and then cohesively through video vignettes/cut scenes.

A description of the project and lessons learned will be briefly discussed, and then a course demo will be provided.

Albert Lewis, CISSP, CISM, HP Enterprise Services

Al Lewis is a cyber security educator and consultant currently serving as a member of the adjunct faculty at Johns Hopkins University and as a senior solution architect for HP Enterprise Services (U.S. Public Sector). Al has taught graduate and undergraduate courses in cyber security and IT audit at JHU since 2006. Al has an MS in Information Systems Management from Johns Hopkins University and is a charter member of JHU's IT honor society. He was elected to the Executive Board in March 2010 at the FISSEA 23rd Annual Conference.

Abstract: Social Insecurity – Social Media Challenges for Cyber Security Professionals

Although social media can be a powerful tool for collaboration and information sharing, it can also expose individuals and organizations to a growing number security threats. This discussion will cover a brief survey of the state of social media today from a security practitioner's perspective and offer thoughts and guidance on a taking an informed approach to use of social media within the workplace and at home.

Wednesday, March 16, 2011 – Vendor Exhibit Day

8:00 – 8:45 am	Registration, Breakfast, and Networking
8:45 – 9:00 am	Morning Announcements Daily Announcers: Louis Numkin (Track 1) and Gretchen Morris (Track 2)
9:00 – 9:45 am	Keynote Address: Green Auditorium Staying Safe in Cyberspace Barbara Lawrence, Northrop Grumman

Keynote: Barbara Lawrence, Northrop Grumman

Barbara Lawrence has more than 25 years of Information Security experience managing Networks, Security and Internet Services. She has also served as the Electronic Systems Sector Chief Information Security Officer and Director of Security Operations. Barbara is responsible for Northrop Grumman's strategies for countering the Advanced Persistent Threat. She is also responsible for governance within the Identity Management Program, serves as the Northrop Grumman CertiPath Policy Management Authority chairperson and is the Designated Approval Authority for the corporate Identity Management program.

Barbara has served as the Northrop Grumman representative for the President's Partnership for Critical Infrastructure Protection, an industry consultant to DoE's Computer Incident Analysis Center, the Information Technology Association of America's InfoSec Committee and NSA's Information Assurance Technical Framework Forum. She currently sits on the Defense Industrial Base's Technology & Architecture Working

Group, the Transglobal Secure Collaboration Program's Cyber Security Working Group and industry's CertiPath Policy Management Authority.

	TRACK 1: Green Auditorium Bridging to the Future – Emerging Trends in Cybersecurity	TRACK 2: Lecture Room B Open Forum
9:45 – 10:15 am	Building a Cybersecurity Talent Pipeline - Tim McManus, Partnership for Public Service	Cyberbullying: The Impact of Staying Connected Dr. Karen Paullet, American Public University
10:15 – 10:40 am	Morning Exhibit Hall Break: Flag Hallway (Exhibit Hall Open 10:30 – 4:00 pm) The vendor exhibit is only one day – Wednesday. Ask FBC for their exhibitor program.	

Tim McManus, Vice President, Education and Outreach, Partnership for Public Service

Tim McManus joined the Partnership for Public Service as Vice President, Education and Outreach in June 2006. Tim is responsible for leading the Partnership's efforts to ensure that government has the talent it needs to meet our county's challenges, including working with a network of more than 730 universities and 80 federal agencies.

Prior to joining the Partnership he served as Director of Marketing for the Corporation for National and Community Service, the federal agency that administers Senior Corps, AmeriCorps, and Learn and Serve America. In that capacity, Tim was responsible for the development and implementation of national marketing, recruitment, and outreach strategies designed to engage Americans of all ages and backgrounds in service.

Prior to his federal service with the Corporation, Tim worked for 17 years in the nonprofit sector. McManus served as Associate Director of Marketing for the National Association of Secondary School Principals (NASSP)—the nation's largest school leadership organization and sponsor of the National Honor Society, National Junior Honor Society, and National Association of Student Councils. Tim also worked with two national civic education and youth leadership organizations, Presidential Classroom, where he served as director of marketing, and the Close Up Foundation, where he served in numerous marketing and management positions.

Tim is active in a variety of volunteer activities, community boards, and professional organizations. A graduate of St. Olaf College, McManus received a B.A. in history and social studies education.

Abstract: Building a Cybersecurity Talent Pipeline

The Partnership for Public Service is a non-profit, nonpartisan organization that works to revitalize our federal government by inspiring a new generation to serve and by transforming the way government works. To accomplish these goals, the Partnership works with colleges and universities across the country to ensure that students are knowledgeable about opportunities in federal service through the *Call to Serve* program. In addition, the Partnership engages with federal agencies to develop innovative recruiting methods and effective hiring techniques to improve government's capacity to build the workforce it needs. Currently, our *Call to Serve* network consists of more than 740 schools and more than 80 federal agencies.

The Partnership's research demonstrates that there could be an IT pipeline problem. A 2009 report "Great Expectations" found only 13% of IT majors view Government/Public Service as an ideal industry. Later that year, the Partnership interviewed and surveyed dozens of federal HR and hiring managers around the cybersecurity field and published "Cyber Insecurity: Strengthening the Federal Cybersecurity Workforce" that highlighted several opportunities to build new talent pipelines. Since then, the organization has worked with several agencies and universities to build IT pipelines through the *FedRecruit* program. In this presentation, Tim McManus will discuss how agencies and campuses have built strong partnerships with university and college campuses. By engaging in a long-term relationship, agencies can access interns and entry-level talent, build on-campus allies, and even influence curriculum.

Dr. Karen Paullet, Associate Professor, American Public University

Karen Paullet received her BS in Information Systems, her MS in Communications and Information Systems and her DSc in Information Systems and Communications from Robert Morris University. Her dissertation was An Exploratory Study of Cyberstalking; Students and Law Enforcement in Allegheny County, Pennsylvania. She received an award for Academic Excellence and Learning from Robert Morris University upon completion of the doctorate.

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), Conference on Information Systems Applied Research (CONISAR) and The Institute for Operations Research and the Management Sciences (SEInforms).

Karen is currently employed by the Allegheny County District Attorney's Office. She has spent over 13 years working with law enforcement preparing cases using digital evidence for trial. She has also taught Information Systems at Robert Morris University since May 2007.

She has spoken at over 100 engagements throughout Pennsylvania on the CSI Effect, the Dangers of Social Network Sites, Cyberbullying and Cyberstalking. She brings her professional experience in law enforcement and teaching to serve as an Associate Professor in the Information Technology Department. In April of 2011 Dr. Paullet will launch a state wide program on Internet Safety for the Pennsylvania Chapter of Children's Advocacy Centers Multidisciplinary Teams. The program will train 1000 trainers throughout the state of Pennsylvania.

Abstract: Cyberbullying: The Impact of Staying Connected

The rapid change in technology and exponential growth in the use of the Internet have resulted in an increase in the number of computer and technology related crimes. Cyberbullying, which occurs when younger people under the age of 18 use technology as an instrument to harass or threaten their peers has become not only a national, but an international problem. In order to fully understand cyberbullying, it is critical that adults and children understand the consequences that occur from inappropriate communication taking place in the digital world. It is imperative that parents, educators and law enforcement work together to stop this growing problem.

	TRACK 1: Green Auditorium Bridging to the Future – Emerging Trends in Cybersecurity	TRACK 2: Lecture Room B Open Forum
10:40 – 11:30 am	Keeping the Lights On: The Challenges of Cyber-security Training and Awareness for the Smart Grid Susan Farrand, U.S. Department of Energy	Cyber Educators: The Lifeline to a Workforce in Crisis Marc H. Noble, (ISC)2

Susan Farrand, Division Director, U.S. Department of Energy

Susan Farrand, CGEIT, is the Director for Policy, Guidance, and Planning in the Office of the Associate CIO for Cyber Security, U.S. Department of Energy. In this position, she also provides Department-level leadership for cybersecurity training and awareness, which includes the development of an enterprise Essential Body of Knowledge, competency matrixes, and functional role curriculum. She is currently working on strategic initiatives for transitioning cybersecurity to the integrated Smart Grid digital technologies. Sue has more than 26 years experience with the Department in both Federal and contractor positions, specializing in cyber security, information architecture, and policy development. Ms. Farrand has an extensive background in training and curriculum development. She was a corporate trainer for Allstate Insurance Company, a curriculum developer for Sargent-Welch Scientific Company, and a classroom teacher. She holds Bachelor of Arts degrees in English and Mathematics and a Master of Arts in Organizational Management and is a Partnership for Public Service Senior Fellow for Excellence in Government.

Abstract: Keeping the Lights On: The Challenges of Cybersecurity Training and Awareness for the Smart Grid

Cybersecurity capabilities are essential to achieving business missions of the Smart Grid. Safe, secure, reliable delivery of electrical power requires a knowledgeable consumer base and skilled industry workforce to perform management and operations activities that are heavily dependent on information resources and rapidly evolving Smart Grid technology. People, as users and creators of information and technology-based systems, are critical to the security of any technological environment. The Smart Grid "people factor" is two-fold; its technology functionality relies heavily on a human network of workers, who need enhanced skills and knowledge to perform their jobs properly, and energy consumers, who need appropriate knowledge and understanding to make effective use of Smart Grid tools and resources. There is a need to educate and persuade people to think and act in a security-conscious way. To protect the grid and the data that flows across it, all users in this human network, from electrical generation to consumption, must have timely, relevant, and easily accessible information concerning their responsibilities and the cyber risks and vulnerabilities that could impact energy reliability and availability. Knowledge and skill development must be addressed through

awareness, training, and education strategies that reinforce cybersecurity responsibilities, build technical competency, and protect the integrity and availability of Smart Grid resources. All stakeholders must be involved in the design and operation of secure systems, communicate effectively about risks, and understand their roles and responsibilities in managing it.

This presentation will discuss the increasing use of information technology, the need for cybersecurity, and the training concerns relative to evolution of the Smart Grid. Four particular concerns of cybersecurity training and awareness will be discussed.

- Recruiting and Retaining a Skilled Cybersecurity Workforce
- Increasing Public Awareness
- Promoting Stakeholder Awareness, Training, and Education
- Expanding Communications and Outreach among Stakeholders

Marc H. Noble, CISSP-ISSAP, CISM, NSA-IAM, MBCI, Director of Government Affairs (ISC)2

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.

Abstract: Cyber Educators: The Lifeline to a Workforce in Crisis

It is clear that there is a critical shortage of U.S. federal information security professionals. As Congress weighs the best way to enhance the capabilities of the workforce, recommendations have been made to identify the best approach. Cybersecurity educators are being recognized as a critical partner in solving this challenge. This session will evaluate the evolving role that cybersecurity educators, their respective institutions and academic programs play in solving the human capital crisis in federal cybersecurity.

	TRACK 1: Green Auditorium Bridging to the Future – Emerging Trends in Cybersecurity	TRACK 2: Lecture Room B Open Forum
11:35 - 12:00 pm	U.S. Cyber Challenge: Developing the Next Generation of Cyber Guardians Karen S. Evans, U.S. Cyber Challenge	Lessons Learned: A Craft Union/Trade School Approach to Security Practitioner Training James R. Lindley, Internal Revenue Service
12 :00 – 1:30 pm	Dedicated Exhibit Hall Hours – Flag Hallway Lunch Provided – NIST Cafeteria Rear	

Karen S. Evans, National Director, U.S. Cyber Challenge

Karen S. Evans is serving as the National Director for the US Cyber Challenge (USCC). The USCC is the nationwide talent search and skills development program focused specifically on the cyber workforce. She is also an independent consultant in the areas of leadership, management and the strategic use of information technology. She recently retired after nearly 28 years of federal government service with responsibilities ranging from a GS-2 to Presidential Appointee as the Administrator for E-Government and Information Technology at the Office of Management and Budget (OMB) within the Executive Office of the President. She oversaw the federal IT budget of nearly $71 billion which included implementation of IT throughout the federal government. This included advising the Director of OMB on the performance of IT investments, overseeing the development of enterprise architectures within and across the agencies, directing the activities of the Chief Information Officers (CIO) Council, and overseeing the usage of the E-Government Fund to

support interagency partnerships and innovation. She also had responsibilities in the areas of capital planning and investment control, information security, privacy and accessibility of IT for persons with disabilities, and access to, dissemination of, and preservation of government information. Included in her accomplishments are making IPv6, HSPD-12, and SmartBUY (which is leveraging the federal government requirements) a reality; elevating the importance of transparency with the publication of the Management Watch List and High Risk List projects; increasing the focus on cybersecurity to include the Federal Desktop Core Configuration for the government; and balancing the expanded use of technology for citizen services with increasing demands for privacy.

Prior to becoming the Administrator, Ms. Evans was the Chief Information Officer for the Department of Energy. There she was responsible for the design, implementation, and continuing successful operation of IT programs and initiatives throughout the Department and its offices. During this time, she was the Vice-Chairman of the Federal CIO Council. Elected to the post in December 2002, she coordinated the Council's efforts in developing federal IT programs and improving agency information resources practices.

Before joining Energy, she was Director, Information Resources Management Division, Office of Justice Programs (OJP), U.S. Department of Justice, where she was responsible for the management and successful operation of the IT program. OJP's bureaus and offices provide funding opportunities for initiatives such as Safe Schools, Safe Start Program, Community Prosecution, Native American Tribal Courts and other programs of high local, state and national interest. Key accomplishments included the implementation of an on-line grants management system to process grants from discretionary, formula and large block grants programs, to streamlining capabilities to ensure for the expeditious processing of claims benefits to families of public safety officers after the September 11th attacks.

She holds a Bachelor's degree in Chemistry and a Master of Business Administration degree from West Virginia University. She resides in Martinsburg, WV with husband, Randy and her two children, Jake and Samantha.

Abstract: U.S. Cyber Challenge: Developing the Next Generation of Cyber Guardians

Where will the nation get the 20,000 technical security experts the military and industry need to protect their systems and to fight in cyberspace? The U.S. Cyber Challenge is the most promising answer. Thousands of young people have participated in competitions and dozens have attended intensive summer cyber camps in CA, DE, and NY. This year all states will be eligible.

James R. Lindley, Senior Secure Software Construction Analyst, Internal Revenue Service

James R. Lindley is a Senior Computer Engineer and Senior Secure Software Construction Analyst for the Internal Revenue Service Cybersecurity Penetration Testing and Code Analysis team, a group charged with performing static source code security analyses and dynamic application-focused testing.

Previously, he was employed by GuardedNet Inc. of Atlanta GA as the Director of Training and by Internet Security Systems Inc. (ISS) of Atlanta as the Senior Security and Products Instructor, the X-Force Anomaly Detection and Remediation Expert, and as Director of Internal Training for ISS Global Managed Security Services. Both firms are now part of IBM. Prior to joining ISS in 1999, Mr. Lindley retired from the U.S. Army as a Chief Warrant Officer, Fourth Class, while serving as Systems Integration Management Officer and Automated Intelligence Processing Officer for the Deputy Chief of Staff for Intelligence of the U.S. Army Reserve Command in Atlanta GA. Other U.S. Army positions include the Chief of the Automation Services Division for the Chief of Staff for Information Management of the 90th U.S. Army Reserve Command in San Antonio TX, and Senior Intelligence Instructor for Interrogation, Intelligence Analysis, and Psychological Operations at the U.S. Army Reserve Intelligence Support Center at Fort Dix NJ. He has served in the U.S. Army as a telegrapher, radio communications specialist, nuclear artillery survey mathematician, training officer, Civil Affairs broadcast supervisor, intelligence analyst, Psychological Operations team chief, interrogator, information automation officer, and as a Senior Military Instructor in a wide variety of military intelligence, security, and computer courses, primarily at the First U.S. Army Intelligence School at Fort Bragg NC. Mr. Lindley also spent over a decade in the broadcasting industry as a writer, talk-show host, news director, program director, and chief engineer. He has held other positions in other career fields.

Mr. Lindley holds an Associate of Arts in ADP from Monterey Peninsula College of Monterey CA, a Bachelor of Science in Liberal Studies from Excelsior College of The University of the State of New York in Albany NY, and a Master of Science in Computer

Science from Southern Polytechnic State University of Marietta GA. He has additional graduate course work in Computer Resource Management at Webster University of St. Louis MO, and undergraduate work in Auditing and Business Management from University of Delaware in Newark DE, and Forensics from the University of Southern Mississippi in Hattiesburg MS. Mr. Lindley holds a diploma in Russian and a diploma with honors in Czech and Slovak from the Defense Language Institute Foreign Language Center in Monterey CA. He also holds a large number of civilian and military training course diplomas and certificates, including a diploma in Broadcast Electronics from Cleveland Institute of Electronics in Cleveland OH. He has served as a speech arts instructor at the University of Southern Mississippi in Hattiesburg MS, a political science instructor at Delaware Technical and Community College in Wilmington DE, an Audio-Visual Arts instructor at the University of Delaware's College of Education in Newark DE, and an Adjunct Professor of Computer Science at Southern Polytechnic State University in Marietta GA and Anne Arundel Community College in Arnold MD..

Among other professional certifications, Mr. Lindley is a Certified Information Systems Security Professional (CISSP) with additional $(ISC)^2$ certifications as an Information Systems Security Architectural Professional (ISSAP), an Information Systems Security Engineering Professional (ISSEP), and an Information Systems Security Management Professional (ISSMP). He is a Certified Secure Software Lifecycle Professional (CSSLP), a Certified Information Systems Auditor (CISA), a Project Management Professional (PMP), a Systems Security Engineering Capability Maturity Model (SSE-CMM) Appraiser, Certified in Homeland Security at Level III (CHS-III), Certified C Programmer by the Institute of Certified Computer Professionals (ICCP), Committee on National Security Systems (CNSS 4013) System Administrator Certified, and A+ and Security+ certified by the Computer Technology Industry Association (CompTIA). He has formerly held a First Class Radiotelephony Engineer Certificate from the Federal Communications Commission and has additional certifications as a Microsoft Certified System Engineer (MCSE), a Microsoft Certified Trainer (MCT), and a Certified Novell Engineer (CNE). Mr. Lindley is a member of the American College of Forensic Examiners Institute of Forensic Science (AFCEI), the Information Security Audit and Control Association (ISACA), the Information Systems Security Association (ISSA), the International Systems Security Engineering Association (ISSEA), the International Information Systems Forensics Association (IISFA), the Project Management Institute (PMI), the Institute of Electrical and Electronic Engineers (IEEE), the American Society for Quality (ASQ), the United States Army Warrant Officers Association (USAWOA), and the Pi Kappa Delta National Honorary Forensics Society.

Mr. Lindley's hobbies are reading, computer programming, carpentry, and gardening. He is currently studying many information technology subjects. He is owned and operated by one wife, two daughters, two granddaughters, and two dogs.

Abstract: Lessons Learned: A Craft Union/Trade School Approach to Security Practitioner Training

Building on continuing efforts by federal agencies to define an information technology (IT) security work force improvement program based on role definitions, the presentation describes some of the lack of adequate detail in defining specialized IT security roles, especially as understood by managers without a security background or training.

The presentation discusses operational roles for security practitioners. There is special focus on the training approaches for the various practitioner roles in managed security services and secure software construction analysis.

The presenter draws on more than three decades in the security arena to support a craft union/trade school approach to training highly specialized security practitioners.

From Wikipedia: Craft unionism refers to organizing … workers in a particular industry along the lines of the particular craft or trade that they work in by class or skill level. It contrasts with industrial unionism, in which all workers in the same industry are organized into the same union, regardless of differences in skill.

The presenter makes a series of suggestions for the appropriate psychologies and skill sets required for security practitioners in the variously defined security "crafts". The presenter will point out those details in role definitions that illustrate the increasing specialization of IT security discipline practitioners, so that the audience will have a better understanding of the difficulty and expected lack of success in proposing role-based training based on inadequately detailed role definitions.

	TRACK 1: Green Auditorium Bridging to the Future – Emerging Trends in Cybersecurity	TRACK 2: Lecture Room B Open Forum
1:30 – 2:20 pm	Federal Virtual Training Environment (FedVTE) and Federal Cybersecurity Training Exercise (FedCTE) Benjamin Scribner, Department of Homeland Security; Hassan Gharekhanloo, Department of State, and Clifford	Improved Customer Service: A Security Trend we Really Need John O'Leary, O'Leary Management Education

	Caughman, Department of State	
2:20 – 2:40 pm	Afternoon Exhibit Break - Dedicated Exhibit Hall Hours – Flag Hallway	
2:40 – 2:50 pm	Door Prizes	

Benjamin Scribner, Department of Homeland Security

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.

Abstract: Federal Virtual Training Environment (VTE) and Federal Cybersecurity Training Exercise (CTE)

The Federal Virtual Training Environment (FedVTE) will provide government-wide, online, and on-demand access to role-based, IT security training and hands-on labs without per seat license fees. This is a mature DoD technology, developed by Carnegie Mellon University/Software Engineering Institute, that is being expanded to supplement existing Federal Agency training. The content library currently holds over 800 hours of captured classroom training and more than 75 hands-on labs.

The Federal Cyber Training Exercise (FedCTE) program will provide government-wide access to experiential and interactive cybersecurity training activities. Training events will be scheduled throughout the year to supplement existing Agency training. Participants will build, refine, and maintain their knowledge and skills through hands-on application of learning concepts in a simulated environment where they can practice attack and defend scenarios. The interactive environment will also facilitate inter-agency collaboration and cross-governmental sharing of best practices. The first FedCTE event took place in Q4 FY 2010 with 68 participants from 25 agencies and 38 cities.

John O'Leary, CISSP, O'Leary Management Education

John G. O'Leary, CISSP, is President of O'Leary Management Education. A computer security practitioner since the 1970's, he has designed, implemented, maintained and managed security for networks ranging from single-site to multi-national, LAN to WAN; including environments connected to the Internet, Intranets, Extranets, Websites, each other, and who knows what else. His background spans programming, systems analysis, auditing, project management, operations and quality assurance, with requisite doses of harmonious, rewarding teamwork and savage corporate infighting. John built and taught one of the USA's first graduate-level university courses in Computer Security at the University of Texas at Dallas in 1976. He has trained tens of thousands of computer security practitioners worldwide in multiple aspects of the field. He is the winner of the 2004 COSAC Award and the 2006 EuroSec Prix de Fidelite. As of this year's FISSEA conference, he has not yet been convicted of anything really serious or run for public office.

Abstract: Improved Customer Service: A Security Trend We Really Need

To successfully bridge us to the future, there is a trend that needs to gain attention, traction and momentum in our profession. Too often, we security people have served our customers (yes, that's right, those sometimes-pain-in-the-neck users are actually our customers) with something less than courtesy and empathetic understanding. We might have gotten rid of them quickly that time, but we also may have left a bad taste with them for future dealings with any security function. Granted, IT security professionals do not have it easy. We must serve our internal and external customers well while providing appropriate security. But don't even think of slowing down crucial business processes. And isn't the customer always right?

An adversarial relationship with our customers makes the bridge to the future rickety and unstable, rife with potholes and deteriorating cables. Good IT security customer service can smooth the roadway and solidify the bridge.

We'll analyze the situation on both the service provider (that's us) and customer sides, emphasizing the need to understand the viewpoints of those we must serve and deal with. We will also analyze complications and particular difficulties inherent in doing

anything that provokes as many potential conflicts as IT security. Customers want what they want, they want it now, and they don't want to hear that what they want represents a significant risk to the organization. We have to remember the function of the agency or business, and we want to serve our customers well, but we also understand that our responsibilities as security professionals are to safeguard organizational assets. And sometimes that means protecting users from themselves. In this session we'll provide specific recommendations for actions that will help IT Security fit established customer service principles and resolve conflicts while continuing to provide appropriate security for our organizations.

	TRACK 1: Green Auditorium Bridging to the Future – Emerging Trends in Cybersecurity	TRACK 2: Lecture Room B Open Forum
2:50 –3:15 pm	Diplomatic Cybersecurity Workforce – Building for the Future Susan Hansche, Avaya Government Solutions and Mike Riley, Edgesource Corporation	Spiral Learning: Cybersecurity Woven into the Organization Corey D. Schou, Informatics Research Institute, Idaho State University

Susan Hansche, Program Director IA Training, Avaya Government Solutions

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.

Mike Riley, ISS LOB Manager, Edgesource Corporation

Mike Riley is the Information Systems Security Line of Business (ISS LOB) Manager for Edgesource Corporation. He supports the Department of State, Diplomatic Security Training Center's (DSTC) Information Assurance program. In July 2010, the Department of Homeland Security certified the DSTC as an ISS LOB Tier II Shared Service Provider of information security role-based training. This certification allows the DSTC to offer courses to improve information and systems security in the federal government by educating information technology professionals with significant security responsibilities.

He retired from the Marine Corps in June 2010, with 31 years of combined active and Reserve duty. As a Reservist, he was employed as a staff member for a US Representative, and also served as a Town Manager. Following the events of September 11, 2001, he was ordered to active duty to address emergency preparedness and crisis response measures for Marine Corps elements in the National Capital Region. Prior to retirement, he was deployed to the Iraqi Theatre of Operations where he supported the II Marine Expeditionary Force (Forward) as the Senior Liaison Officer to United States Forces – Iraq.

Abstract: Diplomatic Cybersecurity Workforce – Building for the Future

We hope you will join us to learn what is new for the Department of State role-based training. We will discuss (a) the methodology State Department is using to identify the cybersecurity workforce, what training is needed, and how it will be tracked; (b) the full suite of instructor-led courses (over 15 new courses expected by FY12); (c) methods to provide interactive virtual instructor-led training, and (d) what is new and exciting in our ISS LOB program.

Corey D. Schou, University Professor, Informatics Research Institute, Idaho State University

Dr. Schou is The University Professor of Informatics, Professor of Computer Science and Professor of Information Systems. He serves as the director of the Informatics Research Institute and National Information Assurance Training and Education Center (NIATEC).

Under his leadership, the Information Systems program was designated the National Center of Excellence in Information Assurance Education by NSA/DHS. His research and publication interests include information security and privacy, ethics, collaborative decision making, the impact of technology on organization structure, and the application of technology to managerial decision making. His work has resulted in over 300 monographs, books articles and formal presentations.

Using collaborative tools he designed for curriculum development, he compiled and edited computer security training materials and standards for the Department of Defense and the National Institute of Standards. These have now been adopted across the federal government. He also serves as the editor of two journals and is the Information Assurance Series editor for a major publisher. Dr. Schou has designed and developed management information and training systems for organizations as diverse as the Federal Express, Microsoft, Florida Parole Commission, American Bankers Association, Industrial Boiler, and General Motors. He works closely with senior management at Apple Computer, Microsoft, United Airlines and other major corporations. His consulting and training has been characterized as being highly personalized and results in a mentoring relationship.

In 2003, Dr. Schou was appointed as the University Professor of Informatics and in 2002 Dr. Schou was selected as the Outstanding Public Servant for his sustained contributions to the academy. Dr. Schou was the 2001 recipient of the (ISC)2 Tipton award for outstanding contribution to the computer security discipline. He was selected as the 1996 Educator of the Year by the Federal Information Systems Security Educators Association and the ISSA service award. In 1997 he received the TechLearn award for contributions to distance education. He has been selected twice by his college as researcher of the year and has been recognized once for his service record.

	Dedicated Exhibit Hall Hours – Flag Hallway - 4:00 pm exhibitor show ends	
	TRACK 1: Green Auditorium Bridging to the Future – Emerging Trends in Cybersecurity	TRACK 2: Lecture Room B Open Forum
3:20 – 4:00 pm	Competency Driven Training Programs Terri Cinnamon, Department of Veterans Affairs	Security Awareness at the Bureau of the Public Debt David Kurtz, Bureau of the Public Debt

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

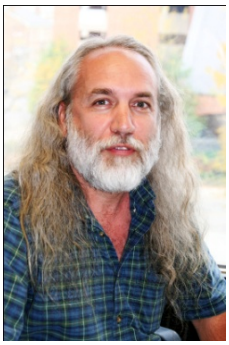
Terri Cinnamon is the Director of Information Technology Workforce Development for the Office of Information and Technology at the Department of Veterans Affairs. A graduate from Wheeling Jesuit University, Terri joined the Department of Veterans Affairs in 1992. During her 19 years with VA, she has 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. Terri has 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 Learning Management System (LMS). Terri and her team 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.

Abstract: Competency Driven Training Programs

Are you providing the right training to the right person at the right time? As Federal organizations adapt to increased pressure to perform at consistently higher levels with finite resources, competency models provide an effective means for agencies to target appropriate professional development opportunities for IT security staff that align with agency goals. Competency models support the human capital life cycle by providing a basis for targeted learning plans and performance measures, yielding more a more skilled workforce, effective recruiting and hiring efforts and determining wiser use of limited training dollars. Come learn how implementing role-based competency models through a learning management system (LMS) provides several simultaneous benefits -- a method to communicate proficiency expectations as well as learning opportunities to staff; ability to monitor performance improvement and progression; to track training completion; and to document regulatory compliance activities.

The Department of Veterans Affairs, Office of Information & Technology (OI&T), IT Workforce Development (ITWD) team has proven to be a leader within the Federal government in successfully implementing competency models for IT-related roles. ITWD recently rolled out several customized competency models based on the OPM IT Roadmap for Federal employees. During this presentation, Terri Cinnamon, Director of ITWD for VA OI&T, will provide a comprehensive overview of OI&T's competency model background, approach, and benefits, and will discuss how the program may be applied in your organization.

David Kurtz, Bureau of the Public Debt



David Kurtz works for the OIT Security Program Staff at the Bureau of the Public Debt in Parkersburg, WV. His federal career began as a Presidential Management Intern at NASA Headquarters in Washington, DC. He worked about three years at NASA before transferring to Public Debt in his native state 23 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, and 2010; 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. In his spare time, he teaches American Government and Constitutional Law for WVU-Parkersburg.

Abstract: Security Awareness at the Bureau of the Public Debt

Public Debt has an extensive security awareness program emphasizing continual communication about security topics with employees through a variety of channels (as opposed to a once year on-line tutorial). The frequency of communication is important to keeping security on the minds of our employees, and helps to provide a feedback loop for more newsworthy tips. Plus, we make an effort to use real stories from actual events (thanks to links with our CSIRC program, anti-virus incident alerts, etc.), thus increasing the relevancy to our employees. In addition, our employees are able to apply a number of the strategies we teach to their home computing, which increases the value of our program to them.

Many of our ideas are transferable to other agencies, plus I plan to share some of my favorite resources for keeping abreast of security news. Samples of some of our publications will also be included with my handouts. I don't claim that we are perfect, but hopefully some of the ideas we use may be helpful to others.

Thursday, March 17, 2011

8:00 – 8:45 am	Registration, Breakfast, and Networking
8:45 – 9:00 am	Morning Announcements Daily Announcers: Cheryl Seaman (Track 1) and Lance Kelson (Track 2)
9:00 – 10:00 am	Keynote Address: Green Auditorium Kevin Gates, Professional Staff Member, House Armed Services Committee
10:00 – 10:30 am	CyberWatch: Creating the Next Generation of Cybersecurity Professionals Dr. Margaret Leary, CyberWatch and Dr. Davina Pruitt-Mentle, Educational Technology Policy, Research, and Outreach (ETPRO)
10:30 – 10:45 am	Morning Networking Break

Kevin Gates, Professional Staff Member, House Armed Services Committee

Kevin Gates joined the House Armed Services Committee as a Professional Staff Member in March, 2007 to be responsible for the Information Technology (IT) and cyber operations portfolio, as well as the Science and Technology (S&T) portfolio. Previously, he worked for 8 years at Strategic Analysis, Inc of Arlington, Virginia for a variety of clients within the DoD science & technology community (including DARPA, ONR and the Defense Science Board), as well as the Homeland Security Advanced Research Projects Agency within DHS(S&T) and the intelligence community. He graduated from the University of North Carolina at Chapel Hill with BAs in History and International Studies, and has a MA from Georgetown University's Security Studies Program. He is the co-author of a chapter on critical infrastructure protection in Volume III of Homeland Security: Protecting America's Targets, James Forest (ed.), 2006.

Keynote Abstract:

The speaker will discuss thoughts on pending and future legislation related to cybersecurity and information assurance, as well as other actions that are being contemplated outside of the legislative process. Emphasis will be placed on human capital planning and workforce development issues. While many of the ideas will have broad applicability across the federal government and the private sector, the speaker will place particular emphasis on the impact on the Department of Defense.

Dr. Margaret Leary, CISSP, CIPP/G, Co-Principal Investigator, CyberWatch

Dr. Leary is a Professor of information assurance courses NVCC and George Mason University and is also a senior security consultant for Avaya Government Solutions. She has more than 20 years experience as a Senior Network Engineer and Security Consultant for Federal agencies. She is a Co-Principal Investigator on the NSF-funded CyberWatch grant and also serves on the Alexandria City Council's IT Commission.

Dr. Davina Pruitt-Mentle, Executive Director and Senior Researcher, Educational Technology Policy, Research, and Outreach (ETPRO)

Dr. Pruitt-Mentle has worked in the field of STEM education & educational and cyberawareness research since 1990. She has spent the past 14 years conducting research on student and educator cyberawareness and K-16 cyberethics, safety and security awareness programs, and developing programs to help increase the IS/IA workforce pipeline. She acts as a Co- PI on the NSF-funded CyberWatch ATE Center, PI for the CyberWatch/UMD Digital Forensics Lab, PI of the MD BRAC (Base Realignment and Closure) –EIS-C MD (Expanding IS Capacity in MD), and serves on numerous national, state and local Task Forces and Advisory Boards.

Abstract: CyberWatch: Creating the Next Generation of Cybersecurity Professionals

CyberWatch, a Consortium of 2- and 4-year educational institutions, is an Advanced Technological Education (ATE) Center, headquartered in the Washington, D.C. region and funded by a grant from the National Science Foundation (NSF). This presentation

will focus on our mission to increase the quality and quantity of the cybersecurity workforce in the nation. Through our resources, members have access to information assurance curriculum, program graduates, virtual labs, educational resources (such as the CyberWatch Second Life Island available for hosting training sessions), and professional development opportunities.

	TRACK 1: Green Auditorium Bridging to the Future – Emerging Trends in Cybersecurity	TRACK 2: Lecture Room B Open Forum
10:45 – 11:35 am	Launching a 21st Century Mentor Program: Using Technology to Enhance Workforce Development Rosa Ayer, Department of Veterans Affairs	Tactical and Strategic Visions of Commercial Certifications George Bieber, DoD

Rosa Ayer, MBA, CISSP, Information Security Specialist, Department of Veterans Affairs

Rosa Ayer is an Information Security Specialist at the VA National IT Training Academy, IT Workforce Development, Office of Information and Technology, Department of Veterans Affairs. Rosa started her career with the Department of Veterans Affairs at the Houston, TX VA Medical Center over 21 years ago. She has over 15 years of experience as an IT specialist, and was the first full-time Information Security Officer at the West Palm Beach VA Medical Center, 1995 – 2000. She served as the Veterans Integrated Services Network 8 Information Security Officer from 2000- 2005. From 2005 to present, she continues to work at the National IT Training Academy where she has served as project manager and developer of the Role-Based Training initiative for the department.

Rosa received a BA from Tulane University, New Orleans, LA 1978; an MBA - University of Miami, Coral Gables, FL, 1981; her CISSP – June 2004; and Security+ - December 2010.

Abstract: Launching a 21st Century Mentor Program: Using Technology to Enhance Workforce Development

In May 2010, the Department of Veterans Affairs (VA) launched the Information Security Officer (ISO) Mentoring Program, integrated with the ISO Competency Model, to help new ISOs transition to the VA environment by pairing them with an experienced ISO mentor. The Program is designed to provide an interactive virtual forum where mentors and mentees can transfer knowledge, share best practices, and enhance their understanding of mentoring best practices. Today, it is an active Program with approximately 50 mentors and 50 mentees from across the United States. The feedback received has indicated that the relationships developed through the ISO Mentoring Program have had a positive impact on the career development for both the mentees and mentors.

This session will discuss how the VA has succeeded in creating this program, beginning with the development and release of the Mentoring Agreement, Mentoring Reference Guide, Mentor/Mentee Survey, New ISO Training, Mentor/Coach Training for Supervisors, and leading to the Quarterly Forums for Mentors/Mentees. Given that the Program participants are located in varying geographic locations, VA uses online tools to carry out each phase of the Program. Many features of the SharePoint tool have been utilized by the Program to host the survey, evaluations, and a Mentoring Discussion Board. The Mentoring Discussion Board gives mentors and mentees a place to ask their questions, connect with each other and learn from each other's experiences in this program and as an ISO. LiveMeeting is used to support the Quarterly Forums for the ISOs. Through the use of its various functionalities, whiteboards and polls are utilized to allow the attendees to share what has worked well in their mentoring relationships, additional tools they may need and any concerns they may have. This process has benefited both introverts and extraverts; both groups are put into an environment where they can feel as though their opinions are heard. The information shared on the whiteboards and polls are used to help continuously improve the Program and provide the ISOs with tools that are helpful to them. Lastly, the use of e-mail and instant messaging (IM) has been incorporated into the forums. The instructor encourages mentors and mentees to take the opportunity to have live discussions on topics presented during the Quarterly Forums and to use this throughout their mentor relationship when they cannot meet face to face.

This session will conclude with an interactive conversation about best practices for standing up the program and how they can be modified to each agency. Participants will leave the discussion with tangible actions that they can take back and implement within their own organization.

George Bieber, Director, IA Workforce Improvement Program Defense-wide Information Assurance Program (DIAP), Department of Defense

Mr. George Bieber is Director, IA Workforce Improvement Program, Defense-wide Information Assurance Program (DIAP). In this capacity he has oversight responsibility for all aspects of the Department's IA and cybersecurity education, training, and awareness activities, the DoD IA Scholarship Program, and workforce management issues.

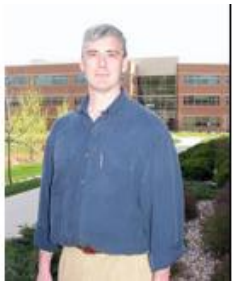
Previously he was Chief, Information Assurance (IA) Education, Training, Awareness (ETA) and Products Branch, Defense Information Systems Agency. He managed the development, production and dissemination of Department of Defense (DOD) IA training and awareness materials.

	TRACK 1: Green Auditorium Bridging to the Future – Emerging Trends in Cybersecurity	TRACK 2: Lecture Room B Open Forum
11:45 – 12:10 pm	Cybersecurity Mystery: Can you solve it in world? Daniel Stein, DHS; Alexander Pyle, USDA; and Susan Hansche, Avaya Government Solutions	Getting Secure Software Assurance Knowledge into Conventional Educational Practice: Three National Initiatives Dan Shoemaker, University of Detroit Mercy
12:10 – 1:15 pm	Lunch Provided – NIST Cafeteria Rear	

Daniel Stein, Program Analyst, Cyber Education & Workforce Development Program, National Cyber Security Division, U.S. Department of Homeland Security

Dan Stein is a Program Analyst in the Department of Homeland Security's National Cyber Security Division, focusing on cybersecurity education, training, and workforce development. Dan has been involved in promoting cybersecurity education efforts in virtual worlds for the past two years. Outside of work, Dan's interests include writing, travel, and the outdoors. Dan received a Bachelor's Degree from the University of Rochester and Masters Degrees from the University of Texas at Austin.

Alexander Pyle, vGov Business Manager, USDA OCIO Enterprise Applications Services



Alexander Pyle is a senior software developer and project manager at the USDA. In his twenty year career at USDA he's worked on diverse systems such as global economic databases, award-winning botanical websites, and the department's ARRA map. An early adapter of the web, he now focuses on virtual worlds and other social media for the Department of Agriculture. Outside of his job he enjoys reading history and volunteering as a system administrator for a local non-profit. Mr. Pyle is a Sun Certified Java Programmer and Project Management Professional. He holds degrees in computer science and history from Colorado State University.

Susan Hansche, Program Director IA Training, Avaya Government Solutions

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.

Abstract: Cybersecurity Mystery: Can you solve it in world?

DHS, USDA and DoS, working together through a partnership, produced a vGov virtual world cybersecurity training module. What started as a concept grew into a virtual world scenario that was developed into a working virtual world prototype. The prototype uses the Teleplace virtual world where the students participate in training using their avatars. The students don on their headsets, sit in front of their computer monitor and immerse themselves into a virtual world not that unlike their own. The virtual world provides an enjoyable way for the students to learn about cybersecurity. The students learn about cybersecurity topics while they try to solve a cybersecurity mystery. A who done it style mystery that requires the students to work in teams while receiving clues in order to solve the mystery, all in the virtual world.

The training is led by an instructor who helps the students out along the way. The students, working in teams, start out in the gathering room, an auditorium style room that contains a big screen that displays a video. The students first learn about the crime they need to solve by watching a video of a young lady named Danielle. Something of Danielle's was stolen and it is up to the teams to figure out what was stolen, how it was stolen and by which crook. The students learn about various cybersecurity topics in the library. They can enter the crook gallery which contains the bios of the potential crooks and important clues. They work in the command center in teams of four and each student has a computer console to receive emails in the virtual world. Some of the emails contain clues, some contain malware, and it is up to the student to figure out which is which. Once their computer is taken over by malware, the students must report the malware to their incident response team in order to reset their computer and continue on with the task. Once the team has correctly solved the mystery they meet back in the gathering room to discuss their findings with the rest of the teams.

Daniel Shoemaker, University of Detroit Mercy

Daniel P Shoemaker, PhD, Principal Investigator and Senior Research Scientist at UDM's Center for Cyber Security and Intelligence Studies. This Center includes the Computer Information Systems-Information Assurance Department, as well as the Center of Academic Excellence for National Security Agency. The Center has just completed a two year Department of Defense Contract to develop Software Assurance Curriculum and Courseware. Dan is a full time Professor at University of Detroit Mercy with 25 of those years as Department Chair. As the Co-Chair for the, National Workforce Training and Education Initiative he is one of the Authors of the National Software Assurance Common Body of Knowledge (CBK) for the Department of Homeland Security. But while Dan spends a lot of time in DC, he is a Michigan man at heart, beginning with his education at the University of Michigan and the outreach opportunities he shepherds within the State of Michigan through his leadership of the International Cyber-Security Education Coalition. This Coalition covers a five state region with research partners as far away as the United Kingdom. Dan also spends his free time authoring some of the leading book in Cyber Security. Look for his newest edition to hit the press, this spring Cyber Security: The Essential Body of Knowledge, based on the DHS National Cyber Security Division's EBOK.

Abstract: Getting Secure Software Assurance Knowledge into Conventional Educational Practice: Three National Initiatives

Given the national priority of secure software, the challenge is to advance software assurance teaching. The problem is that there is currently no single, authoritative point of reference to use to "guide curriculum development for education and training relevant to software assurance" (DHS-CBK, 2006, p. xiv.). As a consequence, secure software assurance topics are taught in a number of disjointed places, including, software engineering, systems engineering, information systems, testing, information assurance, and law. The aim of these three projects is to provide a validated concept and concrete recommendations about curriculum programs and teaching content. A coherent approach will be presented in this session.

This presentation will describe three related efforts to leverage the teaching of secure software assurance content in higher education. All of these were conducted under DoD/DHS sponsorship. The Software Engineering Institute has developed a model reference curriculum for a Masters Degree in Software Assurance, Stevens Institute of Technology has developed two Certificate Programs in software assurance and the University of Detroit has developed detailed teaching content and a wide range of supporting curricular materials for software assurance topics. The outcome is a coherent, top-to-bottom collection of model concepts and concrete recommendations for embedding the discipline of secure software assurance into existing higher education programs

Each of these initiatives has undergone extensive validation, as will be explained in the presentation. The SEI program is a product of an intensive one year effort by a panel of SMEs. It has been fully vetted through national exposure. The UDM material has been vetted through a rigorous Delphi process involving 11 national figures from government, business and higher education. It is also being operationally tested at 15 institutions around the country. The Stevens model has been vetted through exposure at the Department of Homeland Security and SMEs in the Workforce Training and Education Working Group.

As a result, we believe that we have advanced the process of providing new, well-defined and properly validated recommendations for the conduct of secure software assurance teaching. This advice has been supported by extensive study. The intention is to offer a top down presentation from concept to implementation as well as suggestions for how to fit secure software assurance content into established educational settings.

	TRACK 1: Green Auditorium Bridging to the Future – Emerging Trends in Cybersecurity	TRACK 2: Lecture Room B Open Forum
1:15 – 2:05 pm	Information System Technology: When and How to Address Security Implications of New Technologies John Ippolito, Allied Technology, Inc. and Dr. Paul Krasley, DIA	Building and Strengthening a Technical Workforce through Mentoring Kelly Arnold, NSA and Joyce Lusby, NSA

John Ippolito, CISSP, PMP, Allied Technology, Inc.

John Ippolito received a BS degree in Information Systems Management, University of Maryland, 1970. Mr. Ippolito has more than 35 years experience in project management and in design, implementation, and evaluation of large-scale information systems. He has worked with almost every major type of computer and operating system. His Technical experience includes in-depth knowledge of computer and communications security and risk management and risk avoidance. He is a recognized expert in the application of Federal IT security law, policies, and guidelines and has served as an expert witness. He frequently participates on government-industry IT committees and has provided support to a variety of Federal agencies over his 35-year career. He is experienced in the design and review of systems and computer facilities. Mr. Ippolito helped develop and implement FISMA-compliant IT security programs for federal agencies including the Nuclear Regulatory Agency and the Corporation for National and Community Service. He also participated with the Forum of Federal Computer Security Managers which wrote the guidelines for development of IT security plans that ultimately became NIST Special Publication 800-18 and was a named author of NIST Special Publication 800-16. During his government service, he assisted GAO in its initial efforts to standardize the audit/review procedures for IT systems.

Mr. Ippolito is a frequently requested speaker at government and non-government forums, presenting a variety of technical and managerial topics such as designing Internet based applications, selecting the right contract vehicle for IT services, quality assurance and configuration management approaches in client/server environments, and training needs of IT users and professionals. Mr. Ippolito was named Federal Information System Security Educator of the Year for 1997.

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.

Abstract: Information System Technology When and How to Address Security Implications of New Technologies

Information Technology is changing at an increasing rate. Awareness and training must address these new technologies and new uses of existing technologies. This session seeks to provide insight as to when and how new technologies should be integrated into an organization's training program. Hints will also be provided as to how to increase the retention of the risks of these new threats to critical assets.

Kelly Arnold, NSA

Kelly Arnold is a Performance Improvement Consultant working at NSA in the IAD Workforce Development Office. She has 23 years of experience in a variety of operational IA and training positions.

Joyce Lusby, NSA

Joyce Lusby is a Performance Improvement Consultant working at NSA in the IAD Workforce Development Office. She has 25 years of experience working in financial, budget, staff officer, foreign relations and professional development positions.

Abstract: Building and Strengthening a Technical Workforce through Mentoring

This presentation will discuss lessons learned in building a successful mentoring program to support a technical Information Assurance workforce. We will touch on several key steps to include – determining what the workforce wants and needs, building community, training for mentors and mentees, drawing on community resources, and the use of technology to support mentoring activities. The interactive session will end with an actual demonstration of "speed mentoring" – a quick and easy way to link potential mentors with mentees. This technique will allow people to talk with others in the room for about three minutes each about career goals and mentoring styles and needs to see if a "mentor" connection is made. It is almost like speed dating but you can do it at work!

	TRACK 1: Green Auditorium Bridging to the Future – Emerging Trends in Cybersecurity	TRACK 2: Lecture Room B Open Forum
2:15 – 3:05 pm	Securing the Weakest Link Jayson Ferron, Global Knowledge	Workforce Education and Training in Software Security Assurance and Supply Chain Risk Management Joe Jarzombek, National Cyber Security Division, Department of Homeland Security and Robin A. Gandhi, University of Nebraska at Omaha

Jayson Ferron, CEHI, CISM, CISSP, CWSP, MCITP, MCSE, MCT, MVP NSA – IAM *Global Knowledge*

CEHI, CISM, CISSP, CWSP, MCITP, MCSE, MCT, MVP NSA – IAM, Security Practice Lead**.** Jay Ferron brings more than 20 years of experience in security, networking, virtualization, and high performance computing. A multi-faceted author, trainer, speaker, and designer, Jay has led the development of Windows and UNIX security designs, network infrastructures, enterprise designs and installations for numerous Fortune 500 companies as well as government and health agencies.

As president of the Association of Personal Computer User Groups (APCUG), global board director of Global IT Community Association (GITCA), board member of the CT – Information Systems Audit and Control Association, Microsoft Springboard Technical Expert Panel (STEP) member and Microsoft Most Valuable Professional (MVP), Jay is a regular presenter at such prestigious events as COMDEX, Microsoft Tech-Ed, Microsoft Worldwide Partner Conference, Web 2.0 Expo and Summit, and many user groups.

Jay is the author of more than 15 courseware books and papers for Microsoft and other vendors on security, networking, and virtualization technologies. In his current work at Global Knowledge, he is building a unique cyber security program that provides a global perspective of the challenges of designing a secure system. Blog: http://blog.mir.net/

Abstract: Securing the Weakest Link

Network security issues are something organizations are faced with everyday. You can implement technologies such as IDS/IPS and firewalls to help lock down your network. However, have you considered how to protect your networks against non-technical intrusions such as social engineering?

This session will explore 10 things you can do now to help protect and defend your data, network, and personnel against social engineering attacks. During this presentation, we'll discuss the following topics:

- How Easy It is to Gain Information That Can Put You at Risk
- How Social Engineering Can Also Be Done via Technology
- Case Studies and Examples of Techniques That Work to Social Engineer Users

After the session, sample courseware will be available for participants to download and modify.

Joe Jarzombek, PMP, CSSLP, Director for Software Assurance, National Cyber Security Division, Department of Homeland Security

In his role as Director for Software Assurance, Joe Jarzombek leads government interagency public/private collaboration efforts with industry, academia, and standards organizations to shift the security paradigm away from patch management by addressing security needs in work force education and training, more comprehensive diagnostic capabilities, software security automation, and security-enhanced development and acquisition practices.

The National Cyber Security Division (NCSD) of the U.S. Department of Homeland Security (DHS) works collaboratively with public, private, and international entities to secure cyberspace and America's cyber assets. To protect the cyber infrastructure, NCSD has identified two overarching objectives:

- To build and maintain an effective national cyberspace response system
- To implement a cyber-risk management program for the protection of critical infrastructure

Joe served in the U.S. Air Force as a Lieutenant Colonel in program management. After retiring from the Air Force, he worked in the cyber security industry as vice president for product and process engineering. Joe also served in two software-related positions within the Office of the Secretary of Defense prior to accepting his current DHS position.

Robin A. Gandhi, Ph.D., Assistant Professor, University of Nebraska at Omaha

Dr. Gandhi is an Assistant Professor of Information Assurance in the College of Information Science & Technology at the University of Nebraska, Omaha. He received his Bachelors degree from Sardar Patel University, Gujarat, India and his M.S. and Ph.D. from The University of North Carolina at Charlotte. His research interests include information assurance, regulatory requirements modeling and analysis, software engineering, knowledge-intensive software systems, software assurance, certification and accreditation, software metrics and measures, and risk assessment. He is a member of IEEE and ACM professional communities and the DHS Software Assurance Workforce Education and Training Group.

Abstract: Software Assurance Education and Training

With today's global IT software supply chain, project management and software/systems engineering processes must understand how to address security risks posed by exploitable software. Traditionally, these disciplines have not clearly and directly focused on software security risks that can be passed from projects to the organization. Software security assurance processes and practices span development and acquisition and can be used to enhance project management and quality assurance activities. Mr. Jarzombek and Dr. Gandhi explain the critical role of workforce education and training in implementing the practices, guidelines, rules, and principles used to build security into every phase of software development.

	TRACK 1: Green Auditorium Bridging to the Future – Emerging Trends in Cybersecurity	
3:05 – 3:10 pm	Afternoon Networking Break	
3:10 – 3:30 pm	Annual Speak Out: Gretchen Morris, Coordinator	
3:30 – 3:40 pm	Conference Close – Door Prize Drawings	

Annual FISSEA Speak Out

This is an informal session in which anyone can sign up and "speak out" for approximately 5 minutes. Gretchen Morris will coordinate.

- **Speakers for donating their time and knowledge.**
- **Attendees – without You what would be the point?**
- **Participants for entering the Security Contest and sharing posters, trinkets, newsletters, websites, and portions of training programs and Gretchen Morris for coordinating the contest.**
- **Prize Drawing or gift providers:**
  - **SANS Institute, Brian Correia - 3 IPADS and conference bags for attendees**
  - **CompTIA – leather pad folios for attendees**
  - **American Public University – lanyards for attendees**
  - **Potomac Forum, Art Chantker - Potomac Forum scholarship, miscellaneous items, and FISSEA ad in Gov Exec**
  - **Friend of FISSEA – Business books and a Symantec backpack**
  - **Edgewater Federal Solutions – *ISACA Certified Information Security Manager (CISM) Review Manual 2011* and *Official (ISC)2 Guide to the CISSP CBK Second Edition***
  - **Jim Litchko – *2011 FISMA Authorization Process Guide: A Review for the (ISC)2 CAP Certification Exam* and *2011 CAP Exam Sample Questions and Answers***
- **Reginald Leger, Graphic Artist, Avaya Government Solutions for designing the advertising postcards.**
- **Masters of Ceremonies: Cheryl Seaman, Louis Numkin, Gretchen Morris, Albert Lewis, Lance Kelson**
- **Conference Director: Mark Wilson**
- **Conference Assistance: (integral to this effort) Angela Orebaugh, Gretchen Morris, Susan Hansche, Sue Farrand, Pat Toth, Peggy Himes**
- **Program Committee: (additional contributors) Cheryl Seaman, Lance Kelson, Art Chantker, John Ippolito, Marirose Ziebarth, Chris Kelsall, Al Lewis, Richard Kurak**
- **Conference Support: NIST: Mary Lou Norris and Teresa Vicente and the AV team. FBC: Liz Hood, Shannon Grady, Nicole McCracken**