fissea

Federal Information Systems Security Educators' Association

Awareness * Training * Education

27th Annual Conference
March 18-20, 2014

"Partners in Performance:
Shaping the Future of Cybersecurity
Awareness, Education, and Training"

www.csrc.nist.gov/fissea
National Institute of Standards and Technology
100 Bureau Drive, Gaithersburg, MD

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

"Partners in Performance: Shaping the Future of Cybersecurity Awareness, Education, and Training"

27th Annual Conference

Program

updated 12Mar2014

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

Tuesday, March 18, 2014

8:00 – 8:55 am	Registration, Breakfast, and Networking
9:00 – 9:15 am	**Green Auditorium** **Conference Welcome**: Patricia Toth, NIST, FISSEA Conference Director **NIST Welcome:** Donna Dodson, Division Chief, NIST Computer Security Division
9:20 – 10:15 am	**Keynote: Preparing to Defend the Nation in the 21st Century: The Critical Role of Cyber Educators** Dr. Ron Ross, NIST Fellow, Information Technology Lab, Computer Security Division

Donna Dodson Acting Associate Director & Acting Chief Cybersecurity Advisor, Information Technology Laboratory, NIST. She is also the Division Chief of the Computer Security Division (CSD) and the Acting Executive Director of the National Cybersecurity Center of Excellence (NCCoE) at the National Institute of Standards and Technology (NIST). Donna oversees the CSD cybersecurity research program to develop standards, guidelines, technology, tests and metrics for the protection of unclassified Federal information and systems. Through partnerships with industry, Dodson also ensures NIST cybersecurity contributions help secure the Nation's sensitive information and systems. This includes establishing public-private collaborations for accelerating the widespread adoption of integrated cybersecurity tools and technologies.

Dodson received one Department of Commerce Gold Medal and three NIST Bronze Medals. She was a recipient of a 2011 Federal 100 Award for her contributions to advancements in cybersecurity and included in the Top 10 Influential People in Government Information Security.

Keynote: Preparing to Defend the Nation in the 21st Century: The Critical Role of Cyber Educators

Ron Ross is a Fellow at the National Institute of Standards and Technology (NIST). His current focus areas include information security and risk management. Dr. Ross leads the Federal Information Security Management Act (FISMA) Implementation Project, which includes the development of security standards and guidelines for the federal government, contractors, and the United States critical information infrastructure. His publications include Federal Information Processing Standards (FIPS) Publication 199 (security categorization standard), FIPS Publication 200 (security requirements standard), NIST Special Publication (SP) 800-39 (risk management guideline), NIST SP 800-53 (security and privacy controls guideline), NIST SP 800-53A (security assessment guideline), NIST SP 800-37 (security authorization guideline), and NIST SP 800-30 (risk assessment guideline). Dr. Ross is the principal architect of the Risk Management Framework and multi-tiered approach that provides a disciplined and structured methodology for integrating the suite of FISMA standards and guidelines into a comprehensive enterprise-wide security program. Dr. Ross also leads the Joint Task Force Transformation Initiative, an interagency partnership (including NIST, the Department of Defense, the Office of the Director National Intelligence, and the Committee on National Security Systems) that developed a unified information security framework for the federal government.

In addition to his responsibilities at NIST, Dr. Ross supports the U.S. State Department in the international outreach program for information security and critical infrastructure protection. Dr. Ross previously served as the Director of the National Information Assurance Partnership, a joint activity of NIST and the National Security Agency. A graduate of the United States Military Academy at West Point, Dr. Ross served in a variety of leadership and technical positions during his over twenty-year career in the United States Army. While assigned to the National Security Agency, he received the Scientific Achievement Award for his work on an inter-agency national security project and was awarded the Defense Superior Service Medal upon his departure from the agency. Dr. Ross is a three-time recipient of the Federal 100 award for his leadership and technical contributions to critical information security projects affecting the federal government and is a recipient of the Department of Commerce Gold and Silver Medal Awards. Dr. Ross has been inducted into the Information Systems Security Association (ISSA) Hall of Fame and given its highest honor of ISSA Distinguished Fellow. Dr. Ross has also received several private sector cyber security awards and recognition including the Vanguard Chairman's Award, the Symantec Cyber 7 Award, InformationWeek's Government CIO 50 Award, Best of GTRA Award, and the ISACA National Capital Area Conyers Award. During his military career, Dr. Ross served as a White House aide and as a senior technical advisor to the Department of the Army. Dr. Ross is a graduate of the Defense Systems Management College and holds Masters and Ph.D. degrees in Computer Science from the U.S. Naval Postgraduate School specializing in artificial intelligence and robotics.

	TRACK 1: Green Auditorium
10:15 – 10:20 am	Morning Networking Break
10:25 – 11:00 am	**Countering Emerging Threats with an Effective Awareness Program** Karen S. Urban, CISSP, Information Systems Security Manager , K2Share

Countering Emerging Threats with an Effective Awareness Program

The session will open with a discussion on the evolution of technology, threats associated with that technology and how individual behavior can place organizational information and systems at risk. Technology systems are rapidly emerging and existing technologies are being converged to enable the systems to be used in new and innovative ways. Cheaper processors, faster networks, and the rise of mobile devices are driving this technology innovation. Inside the workplace, people are now expecting greater mobility, connectivity and networking capabilities. User-driven mobile trends, such as bring your own device (BYOD) are transforming the business landscape. Many employees have organizational-issued laptops and smart phone, as well as personal mobile device(s). The threat landscape is evolving as rapidly as technology and our dependence on and use of that technology. Whether it's the nation-state sponsored advanced persistent threat (APT) attacks, spear-phishers tricking individuals into revealing sensitive information and intellectual property, or a new strain of malware, we're all surrounded by cyber threats today. Cyber attacks on private, public and government information systems are organized, disciplined, aggressive, sophisticated, and are becoming all too common.

Cybersecurity awareness programs must keep pace with emerging technologies, advanced cyber threats and individual expectations for mobility and access to organizational systems and information. Awareness programs that don't evolve are doomed to fail in preventing a cyber-incidence. This session will provide the audience with proven, cost-effective best practices used in implementing and maintaining an effective cybersecurity awareness program. Best practice awareness programs are effective not only by the subject matter they cover, but by the way they engage individuals in the learning process. If people are not motivated to learn and engage with an awareness course's material, then nothing will be accomplished to reduce organizational risk.

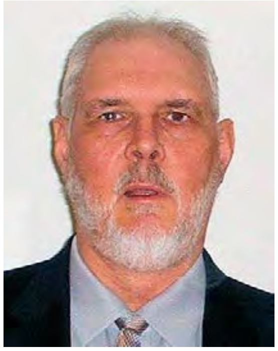
This presentation incorporates real world examples of effective awareness courses and all the necessary considerations for designing cybersecurity awareness programs.

Karen Urban, Information Systems Security Manager at K2Share has over 25 years of experience managing, developing, and supporting a wide range of cyber security and education programs within the federal government and private industry. She is skilled in all aspects of the Security Authorization (formerly C&A), risk assessment, security assessment, penetration testing, system auditing, incident response business continuity planning. She has served as an Information System Security Officer (ISSO) for numerous federal information systems and was selected as the Department of Homeland Security, Federal Emergency Management Agency's ISSO of the year in 2009. Ms. Urban leverages her cyber security expertise to develop educational strategies and programs that focus on reducing cyber risk and modifying user behavior. She is a member of InfraGard, serves as an officer for a local chapter of ISSA and currently holds a number of professional certifications including CISSP, CISA, CRISC, GPEN, GICSP, and PMP.

	TRACK 1: Green Auditorium	
11:05 – 11:40 am	**Developing Construction Workers for Securely Built Software** James R. Lindley, Chief Code Analyst, Penetration Testing and Code Analysis, IRS Cybersecurity	**APUS Multi-Disciplinary Approach to Cybersecurity Education** Dr. Clay Wilson, Program Director, Cybersecurity Studies, The American Public University System

Developing Construction Workers for Securely Built Software

If software security is an emergent quality, from what does that quality emerge? This tutorial presentation is from a course for software project managers by the Penetration Testing and Code Analysis group at the IRS and focuses on the value of secure software construction techniques to project managers. The life cycle phases are described in terms of the skills and psychologies required by the phase practitioners, with a focus on how each practitioner contributes to the emergence of software quality. Special attention is paid to the training and experience required of the various phase practitioners. The educational approach espoused is that of a combination of education, training, and practical experience through apprenticeship, a "blue collar" approach to acquiring "white collar" skills. Since this is a course for project managers, examples are given of the skills and management approaches that benefit successful project completion. Security quality will not emerge unless software project managers recognize and demand the skills and tools relevant to overall software quality.



James R. Lindley is the Team Chief of the Internal Revenue Service Cybersecurity Penetration Testing and Code Analysis team, which performs static source code security analyses and dynamic application-focused testing on IRS applications. In private industry, he has worked for various firms in the information systems security field, as well as taught computer security subjects at several colleges and universities. Mr. Lindley also served for almost 30 years in the U.S. Army in the fields of communications and intelligence, retiring as a senior Chief Warrant Officer.

Mr. Lindley holds an Associate of Arts, a Bachelor of Science, and, and a Master of Science in Computer Science. He has additional graduate course work in Computer Resource Management and undergraduate work in Auditing and Business Management and Forensics. Mr. Lindley holds a diploma in Russian and a diploma with honors in Czech and Slovak from the Defense Language Institute Foreign Language Center.

He is a Certified Information Systems Security Professional (CISSP) with additional CISSP concentrations 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).

The American Public University Multi-Disciplinary Approach to Cybersecurity Education

Cybersecurity concepts and methods change rapidly just as technology itself evolves rapidly. Students who enjoy the challenge and intrigue of how technologies operate to open new possibilities for progress with Information Assurance may be attracted to the traditional Information Assurance (IA) education program. Students who enjoy the challenge of weighing trade-offs to manage the use and direction of current technologies and predict possible future disruptions due to emerging technologies may be attracted to the new APUS Cybersecurity program. Cybersecurity education must evolve to become more multi-disciplinary because all businesses now rely on information technology.

Students should consider whether they are attracted by the intrigue and challenge of technology, or by the challenge of finding trade-offs to manage technology and the challenges for predicting issues and problems related to emerging technologies. Instruction in both the TRADITIONAL IA concentration and the Cybersecurity Program parallel the technology and policy groupings that are found in the 10 domains emphasized by the ISC2. The traditional IA concentration focuses on operation and deployment of technologies, while the Cybersecurity Program courses focus on management of IA technologies. The Cybersecurity Program offers instruction in the human aspects of cyber threats and vulnerabilities. And, while not restricted to non-technical students, the APUS Cybersecurity Program increases the effectiveness of non-technical managers for reducing the level of cyber-risk to their enterprise mission, largely because the courses are multi-disciplinary.

Dr. Clay Wilson is the Program Director for Cybersecurity Studies at the American Public University. The program emphasizes a multi-disciplinary approach to cybersecurity which examines the interconnectedness and complexity of cybersecurity management for both macro- and micro-critical infrastructures. New threats are examined, such as Electromagnetic Pulse and Microwave Directed Energy, along with the vulnerabilities that are targeted by new Advanced Persistent Threats. International issues that present roadblocks to global cooperation for cybersecurity policy are also explored.

Dr. Wilson is past Program Director for Cybersecurity Policy at the University of Maryland University College (UMUC), where he oversaw development of graduate-level courses. Prior to that, Dr. Wilson researched national defense policy at the Congressional Research Service where he analyzed cyber intelligence reports for the U.S. Congress and NATO committees on net-centric warfare, cybersecurity, nanotechnology, and other vulnerabilities of high-technology military systems and critical infrastructures.

Dr. Wilson is a member of the Landau Network Centro Volta, International Working Group, an organization that studies non-proliferation of CBRN and Cyber Weapons. He has moderated panels for the National Nuclear Security Administration on nonproliferation for Cyber Weapons in Como, Italy, and has presented at the China Arms Control and Disarmament Association in Beijing. He has also presented at the US Defense Cyber Investigations Training Academy, at the US National Defense University on the topic of cybercrime, and at the Cyber Conflict Studies Association on the cyber capabilities of terrorist groups. Other projects involved research for Abu Dhabi government officials on computer security and network technology for defense and crisis management while living in the United Arab Emirates. His PhD from George Mason University concentrated on Protection of Intellectual Property

	TRACK 1: Green Auditorium	TRACK 2: Lecture Room B
11:45 – 12:15 pm	**The Technology of Training Tomorrow's Cyber Forces** *(presentation will not be posted)* Dr. Matthew McFadden, Manager / Lead Architect, CSC (Computer Sciences Corp)	**Small Business Cybersecurity and Your Agency** Richard Kissel, NIST

The Technology of Training Tomorrow's Cyber Forces

This session will break down the necessary components of building a cyber-education training system and foster discussion on developing futuristic cyber education training programs of the future and the appropriate technologies that will be required or will be needed. From this session you will learn about technology infrastructure, authentication, learning management systems, content management systems, virtual machines, software development, open source applications, integration, and futuristic technologies to address tomorrow cyber force's needs.

Dr. Matthew McFadden is currently a senior manager and lead architect for CSC developing advanced cyber training solutions for Federal and Defense clients. Additionally, he has worked as research and development lead, instructor, and is a cyber-investigative expert. Also, he has spent several years in the field of information technology specializing in information assurance and security, network intrusion, malware analysis, and forensics. Lastly, Dr. McFadden is a published author and has performed research projects, consulted, presented, and holds numerous industry IT certifications.

Small Business Cybersecurity and Your Agency

The average small business owner/principal in this country is not IT savvy. Since small business use IT, cybersecurity is a requirement not often effectively implemented. Why should you or your agency care?

There are 27 million small businesses in the U.S. That amounts to over 99 percent of all businesses in this country. The small business community produces about 50 % of our GNP. They also generate over 60 % of all new jobs.

They need help to be able to implement an effective cybersecurity program.

What can you do to help? What can your agency do to help?

Richard Kissel, Information Security Analyst, NIST

Richard Kissel is a Senior Information Security Analyst for the National Institute of Standards and Technology in Gaithersburg, MD.

His primary functions at NIST are: (1) Represent NIST in the international standards (ISO/INCITS) arena in the ISO-IEC/JTC1 SC27 - CS1 - Cyber Security technical advisory group and in the ISO-IEC/JTC1 WG6 - CGIT1 – Information Technology Governance technical advisory group; (2) In partnership with the Small Business Administration (SBA) and the Federal Bureau of Investigation (FBI), plan for and conduct information security workshops for small business owners/operators, and; (3) Write information security guidelines for Federal agencies and other NIST customers.

Prior to joining NIST in 2001, he worked as an Information Security Analyst in the Computer Security Office at the SBA. He has worked in the information security profession for over 30 years.

He has earned a B.S. and M.A. (Mathematics Major) from Austin Peay State University. His Information Security certifications include: Certified Information Systems Security Professional (CISSP) and Certified Information Security Manager (CISM).

	TRACK 1: Green Auditorium
12:15 – 1:10 pm	**Lunch Provided – NIST Cafeteria Rear**
1:15 – 1:40 pm Green Auditorium	**Presentation of FISSEA Security Contest Winners** Slide show of all entries prepared by Gretchen Morris, Contest Coordinator **2013 FISSEA Educator of the Year Presentation - *It is a surprise to see who is selected for 2013!*** Presented by J. Paul Wahnish, 2012 FISSEA Educator of the Year. Back up: Susan Hansche, 2011 EOY

	TRACK 1: Green Auditorium	TRACK 2: Lecture Room B
1:45 – 2:25 pm	**Transforming Training to Adapt to the Speed of Change in Cyberspace** Nicole Dean, Raytheon, Moderator; Randall Brooks, Raytheon; Owen Redwood, FSU; Ron Bushar, Mandiant *Panel will not have slides. Q&A session between panelist and moderator.*	**Freely Available e-Resources as Collegiate Textbook in Undergraduate Cybersecurity Program** Dr. Valorie King, Dr. Nancy Landreville , Mr. Ernest Rodgers, Mr. Jeff Tjiputra, and Dr. Richard White, UMUC

Transforming Training to Adapt to the Speed of Change in Cyberspace

The Cyber Community has wrestled with how they will build the core qualifications for cyber operations for nearly a decade. Cyberspace demands the ability to adapt to the speed at which both adversaries' tactics and technologies evolve. Maintaining operational relevancy requires organizations to pace these changes across their workforce. Training must become adaptive, so that leaders, operators and users understand how to counter the threats operating against them. This increasingly evolutionary nature of cyberspace places a premium on identifying processes to infuse training with current operations data. Threat intelligence, vulnerability research and technology forecasts must inform training content and exercise scenarios to ensure your global workforce remains on the cutting edge. State-of-the-art instructional methods and technologies can maximize the training benefit while minimizing time away from the mission. Cyber training at all levels must embrace the new realities of a digital world to be adaptive, innovative, interactive and most importantly, operationally relevant.

This panel will discuss solutions that can keep cyber training operationally relevant through the integration of vulnerability research, threat intelligence and virtual technologies which reach the workforce anytime, anyplace.

Moderator: Nicole Dean, Raytheon; Panel Members: Randall Brooks, Raytheon; Owen Redwood, FSU; Ron Bushar, Mandiant

Randall Brooks, Engineering Fellow, Technical Director Cyber Training, Raytheon, has more than 15 years of experience in Cybersecurity with expertise in Software Assurance (SwA) and secure development life cycles (SDLC). He has been awarded three US patents on Intrusion Detection and Prevention, and three US and one UK patent(s) on Cross Domain solutions. He is also a CISSP, CSSLP, ISSEP, ISSAP and an ISSMP. He is a graduate of Purdue University with a Bachelors of Science from the School of Computer Science. Raytheon is an industry leader in vulnerability research and discovery.

W. Owen Redwood (@sk4ld) is a hacker, teacher, and Ph.D. candidate at the Florida State University focusing his dissertation on "Counter-intelligence tools for Critical Infrastructure for real-time national situational awareness". Owen founded the CTF (Capture the Flag) team n0l3ptr at FSU, which produced many hands on hacking workshops. These workshops developed into a graduate level class that Owen created from scratch and teaches at FSU each spring. The course topics range from security code auditing, reverse engineering, exploit development and vulnerability research, advanced fuzzing, network hacking, web application hacking, penetration testing, and incident response. All students in this class are required to find a 0-day and ethically disclose it. Owen has videotaped every lecture and has produced all the class materials as open-courseware. Other US Universities and even a high school are using the materials for their students, and some are even implementing the same class at their university. Owen frequently travels around the country speaking on how to drastically improve infosec education in the nation.

Ron Bushar is a seasoned, highly effective, and innovative cyber security leader with extensive Federal Government, Cyber Security, Risk Management, and Network Operations experience. Mr. Bushar has over 13 years of experience in the areas of information assurance, information security, cyber operations, and incident response. Prior to his work at Mandiant, Mr. Bushar served as the Director of the Department of Justice Security Operations Center (JSOC). Mr. Bushar has led the Vulnerability Assessment and Penetration Teams, and spent eight years in various cyber operation project management and support roles at ManTech International Corporation. Mr. Bushar began his career in the United States Air Force serving in the Information Warfare Aggressor Squadron at Lackland AFB. Mr. Bushar holds a Master of Science in Management of Information Systems and a Bachelor of Science in Electrical Engineering. He is a certified Project Management Professional (PMP), a Certified Information System Security Professional (CISSP), a Certified Information System Security Architecture Professional (ISSAP), and maintains a professional membership with IEEE.

Panel Moderator: Ms. Nicole Dean is a Director for Cyber Programs, Raytheon Company. Over the past 20 years, Ms. Dean has held increasingly responsible positions in cybersecurity and information technology systems management for Federal, Department of Defense and Intelligence Community cyber and communications systems. Prior to joining Raytheon, Ms. Dean was the Director of the

National Cyber Security Division (NCSD) at the Department of Homeland Security (DHS), as well as the National Cybersecurity Protection System (NCPS) Program Manager, also known as EINSTEIN. As the Director of the DISA Information Systems Center, Ms. Dean oversaw the design, development, and deployment of tools and technologies to enhance and secure the agency's world-wide classified and unclassified networks and information systems, which span 38 locations and support over 8500 users. Dean holds a Bachelor of Science Degree in both Liberal Arts and Information Technology. She holds a Masters degree in Information Systems Security from Colorado Technical University.

Freely Available e-Resources as Collegiate Textbook in Undergraduate Cybersecurity Program

A panel discussion of distinguished faculty from the University of Maryland University College (UMUC) who teach cybersecurity and information assurance. Beginning this spring, the department is moving away from textbooks and embracing e-Resources. Unlike textbooks, e-Resources do not go out of date as fast, cost the students considerably less money, and can originate from a wide variety of sources including NIST Special Publications.

The discussion will center on the different types of e-Resources used in UMUC's Undergraduate courses in the cybersecurity program. Each professor will in turn speak to how different e-Resources are being used to develop course content and facilitate learning. Relevance, sources and currency of information presented as e-Resources will also be discussed.

Of course there are those courses where there is no alternative other than a textbook. Those instances of when a published textbook is more appropriate will be discussed as well. Not infringing on copyrights is a major concern and one where a considerable amount of care is exercised in choosing an e-Resource.

Attendees to this discussion, especially educators will benefit from learning what other resources are out there oftentimes available free of charge. Different NIST publications will be used as examples of how the resources are used. Questions will be answered on where the UMUC panel thinks the use of e-Resources is going and what will the expected impact be to the textbook industry.
The panel, led by Dr. Jeff Tjputra, Academic Director of the Computer Networks & Security and Cybersecurity department all have many years of teaching, industry experience, and advanced certifications in the field of information systems and cybersecurity.

Dr. Valorie King, Dr. Nancy Landreville, Mr. Ernest Rodgers, Mr. Jeff Tjiputra, and Dr. Richard White, University of Maryland University College

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

Dr. King earned the MS in Information Technology degree from UMUC in 2001 and the Doctor of Philosophy degree in Organization & Management (IT Management) from Capella University in 2008. Her dissertation research focused upon e-Government services offered by the 192 UN member nations. She has also earned the *Federal CIO Certification* (UMUC/GSA) and a post-baccalaureate certificate in Health Care Administration (2010) from Capella University's School of Public Service Leadership. Dr. King is a Senior Member of the Institute of Electrical and Electronics Engineers (IEEE) and holds multiple professional certifications including C|EH, CISA, CISM, and CISSP.

Professor Nancy M Landreville is a recognized leader in industry, military, government, and academia. Professor Landreville is frequently requested as a speaker, lecturer, workshop designer, curriculum designer, course developer, consultant in industry best practices, and author. Venues include Academy of Management, International Academy of Management, IEEE (editor and contributing author), ISACA (subject matter expert reviews), ISC2 (contributing editor), GovSec (subject matter expert), National Institute Science and Technology (NIST) (contributor, editor, speaker, consultant), Cap-Sci (author of Geothermal Energy implementation), Cloud Security Alliance (Canada) (speaker), plus Pen-Test magazine and book author on e-discovery. She is one of the officers with the Academy of Management, Organizational Division where she serves as the newsletter editor. She was a presenter at VA's Annual Security Conference on Cloud Computing. Professor Landreville has over a decade in providing consulting services for industry at a level comparable to a government SES; decades of combined military service with the Navy and Army; several decades of higher level government service in information technology; and eight years as a college professor in cybersecurity and information assurance. As a veteran and volunteer with “Bugles across America,” Professor Landreville sounds taps as a volunteer at veteran funerals and other occasions including Memorial and Veterans Day. She has pursued two doctorates simultaneously from 2006 (Doctor of Management and PhD in Applied Management and Decision Science; two Master degrees (Technology Management and Master of Business Administration); two Bachelor degrees (Information Systems Management and Law); several information technology certificates and miscellaneous certifications while working full time and serving her country as a reservist.

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

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

Dr. Richard White has taught data communications and computer security since 2001. He started with UMUC in 2007 as an adjunct professor in the information systems management program. In 2010, he moved to the cybersecurity and information assurance program, where he teaches multiple cybersecurity courses. He serves as the course chair for the CSIA capstone course, Practical Applications in Cybersecurity Management. In addition to teaching for UMUC, he also serves as the Managing Director for Oxford Solutions. Dr. White earned a PhD from Capella University and a MS from UMUC. Prior to his employment at Oxford Solutions, he provided systems engineering and information assurance consultation through Booz Allen Hamilton for the intelligence community, Department of Defense, and civilian agencies of the federal government.

	TRACK 1: Green Auditorium	TRACK 2: Lecture Room B
2:30 – 3:00 pm	**Framework for Improving Critical Infrastructure Cybersecurity** Kevin Stine, NIST	**Awareness vs. Training vs. Education: An Off-Kilter Look** Mark Wilson, Retired Person
3:05 – 3:15 pm	**Afternoon Networking Break/Snack - hallway near Green Auditorium**	

Framework for Improving Critical Infrastructure Cybersecurity

On February 12, 2013, the President issued Executive Order 13636, Improving Critical Infrastructure Cybersecurity, which directed NIST to lead the development of a voluntary framework - based on existing standards, guidelines, and practices - to reduce cyber risks to critical infrastructure. NIST issued version 1.0 of the Framework on February 12, 2014. This session will provide an overview of the Framework and the companion roadmap of cybersecurity activities to be addressed through future public/private collaborations.

Kevin Stine is the Manager of the Security Outreach and Integration Group in NIST's Computer Security Division. The group focuses on the mission-specific application of security standards, guidelines, and technologies to help organizations manage cybersecurity risk. Kevin also recently co-led development of the Framework for Reducing Cyber Risk to Critical Infrastructure which was developed in response to Executive Order 13636. Prior to joining NIST, Kevin was CISO of the Food and Drug Administration.

Awareness vs. Training vs. Education: An Off-Kilter Look

If you are new to the information security (aka, cybersecurity, computer security, et al) profession, or if you have experience but are new to the awareness, training, and / or education aspects of this field, it is important to know the difference between these terms – awareness, training, education. It is important whether you are developing material, writing policy or guidance for consumption by others, or if you are reading and trying to make sense of material written by others. In this session we will discuss awareness, training, and education (and a few related notions), by looking at a non-information security example, and then making a tie-in to the security relevance of each aspect of that example.

Mark Wilson Pre-Retirement Bio: Mark worked at NIST from 1992 until he retired in 2011. He worked on computer security program management issues, including program management reviews, vulnerability analyses and other risk management issues, and security awareness and training.

Mark served as Editor for NIST Special Publication (SP) 800-16 - *Information Technology Security Training Requirements: A Role- and Performance-Based Model* - published in April 1998. He co-authored NIST Special Publication (SP 800-50) - *Building an Information Technology Security Awareness and Training Program* - published in October 2003. He also co-authored NIST Special Publication 800-100 – *Information Security Handbook: A Guide for Managers* – published in October 2006.

Mark also worked closely with the Federal Information Systems Security Educators' Association (FISSEA), was the NIST Liaison to FISSEA, and served on the FISSEA Executive Board for a number of years, including as the Assistant Chair of the Board and as the Chair of the Board.

He earned a B.A. in political science from Old Dominion University in Norfolk in 1983. Mark is a native of New Jersey, a former U.S. Navy journalist, and Vietnam Veteran.

Post-Retirement Bio: Mark is currently working hard to not fail at retirement . . . by not working. He is now paid by Uncle Sam NOT to work, so he is trying hard to stay retired. He smiles a lot more now than he used to while working. He spends his time helping ailing and failing family members, taking long road trips to visit family and friends, and to attend noteworthy sports car races. He is “working” to maintain his shop full of race cars and related projects, and fully intends to get back to racing one or two of them later this year. He is looking forward to warmer weather when he can spend a significant amount of time “working” in his garage / shop, when he is not attacking yard work and house work.

	TRACK 1: Green Auditorium	TRACK 2: Lecture Room B
3:20 – 4:00 pm	**Competency-Driven Simulation Design: Linking Cybersecurity Competition Tasks to Job Performance Models** David Tobey, Indiana University South Bend; Portia Pusey, National CyberWatch Center	**Significant Security Responsibilities and Training** Gretchen Morris, CISSP, DB Consulting Group/NASA IT Security Awareness and Training Center

Competency-Driven Simulation Design: Linking Cybersecurity Competition Tasks to Job Performance Models

As of January 7, 2014, the Department of Homeland Security National Initiative for Cybersecurity Careers and Studies (NICCS) website listed more than 70 different cybersecurity competitions. Although cybersecurity competitions continue to be a popular activity for the development of future cybersecurity professionals, it is not known which competition tasks map to the cybersecurity job tasks which differentiate experts from novices. One way to develop a true understanding of cybersecurity competition task is to map the competition tasks and preparatory activities (practice labs) to existing cybersecurity job performance models. This mapping process can identify of the types of skills required by the competition that indicate mastery and show the extent to which those skills align with job model tasks.

The purpose of the session will be to highlight the process and outcomes of the job performance mapping. We will present lessons learned and will discuss how to apply the mapping process to other competitions. In addition to linking the competition tasks directly to the most important ‘real world’ tasks, the mapping process will also determine the extent to which preparatory activities map to the competitive environment. If implemented on a larger scale, the mapping process provides a common language to compare competition tasks, facilitate alignment between competitions and curriculum to improve competitor preparation and engagement, and can identify skill gaps that produce vulnerabilities in our national infrastructure.

David Tobey, Indiana University South Bend; Portia Pusey, National CyberWatch Center

Dr. David Tobey is a Visiting Assistant Professor at Indiana University South Bend. He also is the founder and Chief Executive Officer of VivoWorks, Inc., a designer of assessment-driven accelerated performance training solutions. Dr. Tobey advises organizations on the development of predictive models of job performance and design, development, and deployment of workforce assessment and development systems. In this capacity, Dr. Tobey served as the Chief Scientist and Director of Research at the National Board of Information Security Examiners supporting fulfillment of their contracts with the Department of Energy and Department of Homeland Security. Dr. Tobey is also the co-founder of Dogs-to-Stars Enterprises LLC and Archemedae Management, Inc., two strategic consulting, business development, and venture capital investment firms.

Dr. Tobey's research into the formation of expertise led to the development of a theory of human performance, the V-to-B Loop, which identifies the cognitive and neurological mechanisms that predict the transition of knowledge into skill. According to this theory, skill develops after sufficient practice leads to the formation of neural clusters deep in the unconscious that execute behavioral programs without the need to recall specific instructions or procedures—the brain's equivalent to a software applet which Dr. Tobey labeled a thinkLet. The formation of thinkLets is detected by a new psychometric technique, Potential Performance Analysis, which NBISE uses to assess the level and potential of cyber security skill development and predict job performance. Prior to joining NBISE Dr. Tobey was a serial entrepreneur whose companies have been listed among INC Magazine's 500 fastest-growing private companies, set international industry standards for systems configuration and integration, and became publicly-traded companies in the early 1990s. He has also served as a consultant, officer and/or board member for private and public companies in the distribution, financial services, hospitality, information technology, life sciences, publishing, and transportation industries.

Dr. Portia Pusey the Director of Instructional Media for the National CyberWatch Center and Senior Researcher with VivoWorks, Inc. She is passionate about serving the mission of improving our national preparedness to protect our digital infrastructure by enriching the engagement and professional skills of cybersecurity learners and professionals. She works with government and private concerns to assess aptitude for careers and contributes to research which accelerate skill development and transfer of knowledge. She leads the design, execution, and analysis of research which strengthens practice in formal and informal cybersecurity learning situations. She specializes in managing discrete project strands to realize a wider program of work which prioritizes differentiating skills in cybersecurity fields. She works with national organizations to develop institutional strategies for research which provide focus responding to funders' solicitations; and leads or contributes to grant writing efforts. With an entrepreneurial background, and formal training in education, she bridges interdisciplinary landscapes to coordinate and support research in cybersecurity education.

Significant Security Responsibilities and Training Discussion

This will be an interactive session (facilitated discussion) designed to enable open conversation about current and potential solutions used to meet the training requirements for those with Significant Security Responsibilities at your Agency. Come and share what your Agency is currently doing to select the audiences and training for those with Significant Security Responsibilities. Hear what your peers are doing and share best practices. Ask questions and work toward possible solutions together. We will also talk about how the selection and/or creation of training may change once the current draft update of the NIST SP 800-16 is finalized (as compared to the original).

Gretchen Morris, CISSP, DB Consulting Group / NASA IT Security Awareness and Training Center. Gretchen Morris has been supporting the NASA IT Security Awareness and Training Center since November 2000. She has over 20 years of teaching and troubleshooting experience on a variety of software packages and hardware configurations. She has a Bachelor of Applied Science in Resource Management degree from Troy State University. She earned the Master Training Specialist designation while serving as a Navy Instructor and has maintained CISSP certification since June 2002.

	TRACK 1: Green Auditorium
4:05 – 4:40 pm	**An Open Discussion: Phishing and Whaling Attacks** Panel Chair: Pat Toth, NIST; Ralph Massaro, Wombat Security Technologies; Roberto Cardona, Systegra; Rashawd D. Smith, MasterSmith Information Security Consulting

An Open Discussion: Phishing and Whaling Attacks

This panel will present an overview of phishing, whaling and spear phishing attacks, Anti-phishing training approaches and techniques will be discussed. Panelists will present approaches to improving the effectiveness of anti-phishing awareness and training programs.

Patricia Toth, NIST, Panel Chair; Ralph Massaro, Wombat Security Technologies; Roberto Cardona, Systegra; Rashawd D. Smith, MasterSmith Information Security Consulting

Pat Toth is a Supervisory Computer Scientist in the Computer Security Division at NIST. Her current project areas include information security, cybersecurity awareness, training and education. Pat is the lead for the FISMA team, Chair of the FISSEA Technical Working Group, and co-author of SP 800-16 rev 1.

Pat has worked on numerous documents and projects during her 20+ years at NIST including the Trust Technology Assessment Program (TTAP), Common Criteria Evaluation and Validation Scheme (CCEVS), Program Chair for the National Computer Security Conference, FISMA family of guidance documents including SP 800-53 and SP 800-53A and the National Initiative for Cybersecurity Education (NICE). She is a recipient of the Department of Commerce Gold and Bronze Medal Awards.

Pat holds a Bachelor of Science in Computer Science and Math from the State University of New York Maritime College. She served in the Navy as a Cryptologic Officer. Pat received a Joint Service Achievement Medal and Defense Meritorious Service Medal for her work on the rainbow series of computer security guidelines while assigned at the National Security Agency.

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

Roberto Cardona, President, Systegra. Mr. Cardona has aided clients in achieving their specific information security goals since 1997. He performs numerous information security services, including: penetration testing, vulnerability assessments, intrusion detection / protection implementation and design, enterprise security monitoring and management (e.g., SIEM), incident response, and security product testing and evaluation. Additionally, he has provided broader support was provided in support of certification and accreditation (C&A) efforts which were based on National Institute of Standards and Technology (NIST) 800 series special publications, and Department of Defense methodologies (DITSCAP/DIACAP). Mr. Cardona led forensic analysis projects of servers and workstations in support of a Department of Justice Investigations. He has had technical experiences with multiple threats and vulnerabilities, and implemented successful mitigation.

Rashawd D. Smith started out in Information Technology in 2006 for the Department of the Interior. From there moving into Help Desk Management for the 2010 Census he found the need for vigilant security in the public and private sectors and chose Systems Security Compliance as his discipline.

Working at STG Inc. he was trained in Security Compliance using the recommendations and guidance. He then performed this duty for Veterans Affairs for more than a year. Afterwards he worked on the other side of compliance as an ISSO to manage security for MicroPact Inc. managing assessment and security for the Software as a Service Company.

Most recently Mr. Smith went on to work as an Information Security Threat Analyst for Visa USA where he analyzed and triaged incoming and outgoing potential and occurring threats for the organization. He is starting his own consulting firm to further his journey into securing information systems.

	TRACK 1: Green Auditorium
4:45 pm	**Door Prizes Drawing - Green Auditorium**
5:00 pm	**Dinner Get Together – Location TBD – Not included in registration fee. Sign-up sheet at desk.**

Wednesday, March 19, 2014

Vendor Exhibition – Flag Hallway – open 10:00 - 2:45

8:00 – 8:50 am	Registration, Breakfast, and Networking (no need to check-in at the registration desk after receiving your badge on first day)
8:50 – 9:00 am	**Green Auditorium** **Welcome/Morning Announcements**: Jim Wiggins, FITSI **Vendor Preview Slide Show**
9:05 – 9:40 am	**Keynote:** Amb. Karen Kornbluh, Executive Vice President of External Affairs for Nielsen, former US Ambassador to the Organization for Economic Cooperation and Development (OECD)
9:45 – 10:25 am	**Opening the Digital Pandora's Box: Mobile Device Security Awareness** Dr. Karen Paullet, American Public University
10:25 – 10:40 am	**Morning Break – Visit with Vendors in Flag Hallway**

Ambassador Karen Kornbluh is Executive Vice President of External Affairs for Nielsen. Appointed to this role in December 2013, Karen is responsible for leading Nielsen's global efforts in key areas, including government and public affairs and services. Previously, Karen was the U.S. Ambassador to the Organization for Economic Co-operation and Development (OECD) from 2009 – 2012. Under her leadership, the US convened government, technology, and business leaders to develop the first global Internet Policymaking Principles. She led efforts to open access to the OECD's data and to strengthen its anticorruption efforts. She worked with former Secretary of State Hillary Clinton to launch both the Gender Initiative and the Middle East-North Africa Women's Business Forum.

Ambassador Kornbluh received her Masters from Harvard University's John F. Kennedy School of Government and her B.A. from Bryn Mawr College.

State Dept.

Opening the Digital Pandora's Box: Mobile Device Security Awareness

The number of mobile phone users, at the end of 2012 was approximately 5.9 billion worldwide (Wireless Intelligence, 2013). Cell phones have become ubiquitous within our society, and many would now consider them a necessity rather than a convenience. People are staying "plugged-in" and connected to what has become an "always on" world. As educators, mobile and wireless devices will continue to become increasingly important tools for accessing information and communicating with their workforce. Proximity has now become inconsequential in terms of interaction. We are now faced with an area of concern on how to keep our mobile devices secure. New ways of abusing wireless and mobile devices to facilitate the commission of technology-enabled incidents and crime continue to emerge. What mechanisms do we have in place to deal with security threats? What are the legal ramifications of BYOD in regards to mobile computing? How can we stay safe while using our mobile devices?

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

10:25– 10:40 am	**Morning Break – Visit with the Vendors in the Flag Hallway** **Vendors will be there from 10:25 – 2:45**

	TRACK 1: Green Auditorium	TRACK 2: Lecture Room B
10:45 – 11:20 am	**Improving IT Security for Geographically Disbursed Communities through Blended Mentorship** Sandra Toner, Technical Specialist, ICF Jacob & Sundstrom	**Continuous Monitoring and Ongoing Authorization** Kelley L. Dempsey, Senior Information Security Specialist, NIST

Improving IT Security for Geographically Disbursed Communities through Blended Mentorship

This presentation will highlight a specific case that demonstrates the evolution of a project over 10 years to provide more efficient, targeted cybersecurity education. Key points include:

- The mentorship relationship and its importance in incrementally improving cybersecurity posture.

- A cost-effective model for reaching a large dispersed audience, which includes virtual mentorship, live instruction, and risk assessment scaffolding.

- Virtual mentors can identify patterns that inform curriculum. This leads to learning that is relevant, focused, and just-in-time.

Sandra Toner, ICF Jacob & Sundstrom

Continuous Monitoring and Ongoing Authorization

This session provide information on the comprehensive Information Security Continuous Monitoring (ISCM) process as described in NIST Special Publication 800-137. ISCM purpose, objectives, policy, specific process steps, automation, and its place within the NIST Risk Management Framework will be discussed.

Kelley L. Dempsey, Senior Information Security Specialist, Information Technology Laboratory/Computer Security Division. Kelley Dempsey began her career in IT in 1986 as an electronics technician repairing computer hardware before moving on to system administration and network management. While with the Department of the Navy, she began focusing on information system security and conducted a large scale DITSCAP certification and accreditation from start to finish. In 2001, Kelley joined the NIST operational Information Security team, managing the NIST information system certification and accreditation program and then joined the NIST Computer Security Division FISMA team in October 2008. Kelley has co-authored NIST SP 800-128 (Security-Focused Configuration Management) and NIST SP 800-137 (Information Security Continuous Monitoring) and is a major contributor to NIST SPs 800-30 Rev 1, 800-37 Rev 1, 800-53 Rev 3/Rev 4, 800-53A Rev 1/Rev 2, and 800-39. Kelley completed a B.S. in Management of Technical Operations, graduating cum laude in December 2003 and is currently working towards an M.S. in Information Security and Assurance. Kelley also earned a CISSP certification in June 2004 and a CAP certification in January 2013.

	TRACK 1: Green Auditorium	TRACK 2: Lecture Room B
11:25 – 12:05 pm	**Fighting the APT: Intelligence, Analysis, and User Awareness** Albert Lewis, CISSP, CISM, CGEIT, InfoSec Policy & Compliance Lead, The MITRE Corporation	**Training Methodologies for Continuous Diagnostics and Mitigation and Ongoing Assessment** Eric Goldstein, Policy Advisor, Department of Homeland Security/Federal Network Resilience

Fighting the APT: Intelligence, Analysis, and User Awareness

Traditional approaches to information security include reducing the attack surface and emphasizing mitigation and compliance. But with today's escalating threats, a shift in traditional thinking is required from information assurance based on static defenses to threat-based defense strategy that balances mitigation with detection and response. This presentation will discuss best practices in developing cyber intelligence founded upon a workforce culture of cyber-awareness and creating an agile defensive posture aligned with relevant threats.

Al Lewis is a cyber security business executive and subject matter expert with a diverse background in security engineering, operations management, regulatory compliance and policy. He has over two decades of leadership experience in information technology, cyber security, and program management, having served all three branches of the federal government. He is an active speaker at industry conferences. In his current role, he serves on MITRE's internal security team leading all information security policy and compliance initiatives for the corporation.

Training Methodologies for Continuous Diagnostics and Mitigation and Ongoing Assessment

The Department of Homeland Security (DHS) established the Continuous Diagnostics and Mitigation (CDM) program to provide federal departments/agencies and state, local, tribal, and territorial (SLTT) governments with continuous diagnostics tools, dashboards, and integration services and enable risk-based, and cost-effective cybersecurity. CDM will further enable network administrators to know the state of their respective networks at any given time and prioritize vulnerabilities and defects based upon the greatest potential risks.

To ensure that CDM is implemented in a standardized and effective manner, and to promote broad recognition and understanding of the CDM program across diverse stakeholders, the Department of Homeland Security is developing a comprehensive training program for federal and SLTT partners. This session will describe the purpose, structure, access, and desired outcomes of the CDM training program. This session will further explain how DHS is developing a comprehensive training program encompassing various platforms, methods, and instructional techniques to maximize both audience exposure and learning outcomes. Students attending this session will gain an improved understanding of the CDM program, will acquire information on accessing and participating in CDM training, and will understand how CDM can enable an effective Information Security and Continuous Monitoring program, per OMB Memorandum 14-03.

Eric Goldstein serves as a Policy Advisor in the Federal Network Resilience (FNR) within the U.S. Department of Homeland Security (DHS). Within FNR, he manages training and governance initiatives for the Continuous Diagnostics and Mitigation (CDM) program. Prior to DHS, he held positions with the Homeland Security Studies and Analysis Institute (HSSAI), focusing on cybersecurity information sharing, performance measurement, and critical infrastructure protection, and in State and local government.

12:05– 1:25 pm	**Lunch Provided in NIST Cafeteria Rear** **Another Chance to Visit the Vendor Exhibits – Flag Hallway**	
	TRACK 1: Green Auditorium	TRACK 2: Lecture Room B
1:30 - 2:20 pm	**Dept. of State Cybersecurity Online Learning Program Demonstration** Mike Riley, Program Manager, Edgesource Corp/DoS; John Light, DoS	**Using the NEW Cybersecurity Workforce Framework** Ben Scribner, DHS

Dept. of State Cybersecurity Online Learning Program Demonstration

The U.S. Department of State (DoS) will demonstrate the capabilities of their Cybersecurity Online Learning (COL) Program by scheduling a live workshop to coincide with the FISSEA Conference. FISSEA attendees will be able to view the live lecture taking place online using Adobe Connect, and also see a demonstration of a live lab activity and the administrative capabilities of the lab tools that we use in some of our workshops. Attendees will have the opportunity to ask questions about the program and see the list of upcoming workshops.

DoS conducts 2-3 workshops per month that last 60-90 minutes. Many of the COL workshops are open to all government agency cybersecurity professionals at **no cost** to the parent agency. We record each workshop and make these recordings available for viewing on our website, at **no cost**. Since all of the workshops/recordings are available on the internet, this program offers great flexibility to our students - they can attend/view from their office, home, and even their mobile device, at **no cost**.

These workshops, though on-line, offer a great amount of interactivity. Our instructors are experienced in this environment and engage the students with directed and poll questions, demonstrations, labs, as well as large and small group discussions.

Our students are also using these workshops for Continuing Professional Education (CPE) units to maintain their professional certifications.

Mike Riley joined Edgesource Corporation in 2010 following his retirement of 31 years with the United States Marine Corps. He is the Program Manager for the Department of State, Information Assurance Branch's training program and also manages the Information Systems Security Line Of Business certified by the Department of Homeland Security as a Center of Excellence for information assurance/security training. Prior to retirement, he stood up and directed a staff that oversaw mission assurance requirements for all Marine Corps elements in the National Capital Region, as well as representing Marine Corps interests as the liaison to the Joint Force Headquarters – National Capital Region. He developed and implemented several programs for mission assurance to include critical infrastructure protection, force protection, anti-terrorism actions, information assurance, and physical security requirements, as well as coordinated interagency collaboration with federal, state, and local government partners.

Using the NEW Cybersecurity Workforce Framework Panel

The National Cybersecurity Workforce Framework (“Framework”) provides educators, managers and training providers with one common definition of cybersecurity work. This common lexicon allows organizations to work together and build the pipeline and career paths for cybersecurity professionals with the right knowledge, skills and abilities. The Office of Personnel Management has mandated that all US Federal departments and agencies to use the track and report their cybersecurity professionals. Educational institutions and training providers are designing their coursework and degree programs to align with the Framework. Come learn about the Framework 2.0 and how it can help your organization to recruit, train and retain the right people with the right knowledge, skills and abilities.

Benjamin Scribner is the Program Director for the DHS National Cybersecurity Professionalization and Workforce Development program. He has ten years of experience leading coalitions of US federal departments and agencies to develop resources for cybersecurity professionals. He led the establishment of the Federal Virtual Training Environment and Training Events program. Mr. Scribner now supervises DHS leadership of the National Initiative for Cybersecurity Education (NICE) and the National Initiative for Cybersecurity Careers and Studies (NICCS).

2:20 – 2:35 pm	**Afternoon Networking Break/Snacks** **Visit Vendors in Flag Hallway (closes after break)**	
	TRACK 1: Green Auditorium	TRACK 2: Lecture Room B
2:40 – 3:05 pm	**Social Engineering: An Update on Attacks and Defenses for your Users** Ralph Massaro, VP of Sales, Wombat Security Technologies	**Defense Against the Dark Arts – Cyber Security Basics** Craig Holcomb, Senior Computer Scientist , NSA

Social Engineering: An Update on Attacks and Defenses for your Users

Are you having trouble keeping up with the latest social engineering attacks? You’re not alone. According to Kaspersky, in 2012-2013, 37.3 million users around the world were subjected to phishing attacks — up 87% from 2011-2012. This doesn’t include all of the other social engineering attack types. Not only are there more attacks, the attacks are getting more sophisticated every day requiring extreme vigilance to avoid attack.

In this session we’ll discuss current attack approaches and make recommendations about how to arm your employees so that they can be aware and defend against these attacks. More sophisticated attack approaches require creative training and education solutions. The days of doing annual PowerPoint presentations or expecting that a series of short videos will make your users more capable to defend against attack are long gone. In this session we will also talk about new approaches to motivating employees to engage and become part of a company’s defenses.

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

Defense Against the Dark Arts – Cyber Security Basics

(Appropriate for grades 9-12) Just as young wizards in the Hogwarts Academy must learn about dark magic and dark creatures to defend themselves, so must young cyber wizards learn about malware and hackers. Topics covered include viruses, worms, Trojan horses, identify theft, phishing and social engineering.

Mr. Craig Holcomb is a Senior Computer Scientist with the National Security Agency. He holds a Bachelor's degree from the University of Tennessee with a double major in Mathematics and Computer Science, a Master's degree in Computer Science from George Washington University, and an Applied Scientist degree also from GW with a major in Computer Science Software and Systems, with minors in Hardware and Artificial Intelligence. Mr. Holcomb has been with NSA for over 32 years. He began his career as a programmer; he later ran a technology lab introducing new computer technology into NSA. He was the technical director for NSA's Chief Information Officer's office of Policy and Governance. He served as a technical recruiter hiring Computer Scientists and Engineers for NSA's Information Assurance Directorate. From there he moved to be the technical director for the Modeling and Simulation Oversight Division in NSA's Operations Research, Modeling and Simulation office. Currently, he's NSA's Senior Compliance Officer, ensuring NSA complies with laws such as the Federal Information Security Management Act.

Mr. Holcomb has been a speaker for NSA's Mathematics Speaker's Bureau for over 17 years. He was the Master Instructor for a course called Operations Research in Real Life at NSA's Math And Related Sciences (MARS) summer camp for high school students. He has created or substantially changed 8 talks and presented 14 of the 52 talks in NSA's catalog to a wide variety of audiences including students in Elementary, Middle and High Schools in both public and private schools, county wide meetings of high school Mathematics Department Heads, and the Maryland Council of Teachers of Mathematics Annual conference. Some of his talks include Cyber Ethics; Cyber Security: Public Key Cryptography & Public Key Infrastructure; Defense Against the Dark Arts - Cyber Security; and Winning Games: Luck or Logic? Mr. Holcomb has been a technical recruiter for over 15 years presenting information on NSA to high school and college students. He represents the skill field of Computer Science and is the Chair of NSA's Stokes Educational Scholarship Program Mentor Committee.

	TRACK 1: Green Auditorium	TRACK 2: Lecture Room B
3:10 – 3:35 pm	**Non-Malicious Security Violations– Mitigating the Threat** Carl D. Willis-Ford, Senior Technical Advisor II, SRA International, Inc.	**NIST SP 800-16 Rev 1, A Role-Based Model for Federal Information Technology/Cyber Security Training** Patricia Toth, Supervisory Computer Scientist, NIST; Penny Klein, Sr. Security Analyst, Systegra

Non-Malicious Security Violations – Mitigating the Threat

Non-Malicious Security Violations (NMSVs) are where employees knowingly violate security policy, not to hurt the agency or help the bad guys, but to make their jobs easier or to help a co-worker. NMSVs are under-represented in most reports, being included in the category of 'accidents', as in the annual Verizon Data Breach Report. This presentation will take a look at common NMSVs, why they occur, and the potential impact. Research in the area (including behavioral frameworks and models) will be discussed at a high level, as will possible approaches for managing the problem.

Carl D. Willis-Ford Currently a Senior Technical Advisor II at SRA International, Inc., doing capture and solution architect work. Formerly a nuclear reactor operator on fast attack submarines in the US Navy. Post-Navy, I taught nuclear reactor theory at Puget Sound Naval Shipyard until moving to IT as a database administrator. I started with SRA in 1997. I have a B.S. in Computer Science (Chapman University), an M.S. in Network Security (Capitol College), and an M.S. in Technology Management (George Mason University) and am currently in a DSc in Information Assurance program at Capitol College. I mentor graduate students in both Technology Management and Management of Secure Information Systems programs at GMU. I've presented on data security, software assurance, social engineering, and security governance topics to International Oracle Users Group conferences, the regional and state Oracle Users Groups, the Executive MBA program at GMU, the IA club at Penn State, and various commercial firms. Awarded for Individual Excellence at SRA for 2013 and named a Senior Member of ISSA in January 2014.

NIST SP 800-16 Rev 1, *A Role-Based Model for Federal Information Technology/Cyber Security Training*

Role-based training is required by FISMA for those individuals who have specific security responsibilities. NIST has the responsibility to provide role-based training guidance. The NIST SP 800-16, Rev 1, A Role-Based Model for Federal Information Technology/Cyber Security Training has been revised and through a public comment period. This presentation will outline the revised document and the methodology; as well as discuss next steps.

Patricia Toth is a Supervisory Computer Scientist in the Computer Security Division at NIST. Her current project areas include information security, cybersecurity awareness, training and education. Pat is the lead for the FISMA team, Chair of the FISSEA Technical Working Group, and co-author of SP 800-16 rev 1.

Pat has worked on numerous documents and projects during her 20+ years at NIST including the Trust Technology Assessment Program (TTAP), Common Criteria Evaluation and Validation Scheme (CCEVS), Program Chair for the National Computer Security Conference, FISMA family of guidance documents including SP 800-53 and SP 800-53A and the National Initiative for Cybersecurity Education (NICE). She is a recipient of the Department of Commerce Gold and Bronze Medal Awards.

Pat holds a Bachelor of Science in Computer Science and Math from the State University of New York Maritime College. She served in the Navy as a Cryptologic Officer. Pat received a Joint Service Achievement Medal and Defense Meritorious Service Medal for her work on the rainbow series of computer security guidelines while assigned at the National Security Agency.

Penny Klein has been in the Information Assurance field for 25+ years. She is a recognized expert in her field. Her career consists of supporting various Department of Defense (DOD) Agencies, Federal Agencies and the Private Sector. Ms. Klein has participated in high level security working groups on multiple information assurance issues. She works for a small business, Systegra, and is currently providing information assurance services to Federal and State Government, as well as Industry clients. These services include policy and FedRAMP documentation development, training and security program consultation.

	TRACK 1: Green Auditorium
3:40 – 4:10 pm	**Adapting and Establishing New Education Strategies to the Continuously Evolving Cyber Terrain** Grayson Koogle, EmeSec, Inc.

Adapting and Establishing New Education Strategies to the Continuously Evolving Cyber Terrain

As cloud and mobile computing technologies continue to evolve, “cyber hackers” are also advancing and improving their strategies and capabilities to breach our critical infrastructures. Strategic forward thinking and proactive approaches to training are required. From this presentation, agencies, cyber professionals and academia in attendance will explore the movement in cyber security training from a stagnant choice (i.e. standard work week classroom training) to more flexible options (i.e. web based online interactive/virtual training) as well as some of the resultant issues. Specifics include approaches to address the workforce culture shift; benefits to implement an online education culture; and how to adapt and take advantage of training opportunities during off-peak hours.

The presenter will address the evolving and continuous threats attacking government agencies and the need to maintain a proactive training environment to constant security training. Attaining and maintaining professional certifications is a business imperative for organizations to show and document their experience and expertise in the understanding of and countering continuous threat to our nation’s most sensitive information.

EmeSec, who holds the highest standards for quality assurance with their ISO 9000, 20000, 27000 certifications, will provide firsthand knowledge on the need for more requirements to maintain currency and certifications on new government systems and applications. Our speaker will also share lessons learned and best practices to establish an education strategy that better fits the agency work environment and strategic mission.

Grayson Koogle came to EmeSec from a senior management position in SAIC. While there, he had responsibility over programs focused in areas such as information technology/assurance, test and evaluation, and international programs.

Mr. Koogle is a retired Navy Surface Warfare Officer with over 20 years of leadership experience. Key assignments ranged from fleet operations to work as the Navy’s Test and Evaluation Coordinator for C3I and Information Systems and Navy Space Test Program Officer. He retired while serving as a professor in the Test and Evaluation Division at the Defense Systems Management College (now Defense Acquisition University) and transitioned into industry.

His industry experience over the past 15 years includes management positions in advanced technology demonstrations and transition, product development, management consultant services, test and evaluation, systems engineering, information technology and information assurance.

4:15 pm	**Door Prizes Drawing - Green Auditorium**

Thursday, March 20, 2014 – *"Gov Poster Session is back"*

	Green Auditorium
8:00 – 8:45 am	**Registration, Breakfast Snack, and Networking - hallway outside Green Auditorium**
8:45 – 8:55 am	**Welcome Day 3 Morning Announcements –**
9:00 – 9:35 am	**Keynote Address:** **Ms. Linda Cureton**, Chief Executive Officer and Founder of Muse Technologies, Inc. (former NASA CIO)
9:40 – 10:15 am	**New Approaches to Security in a Web-Based World** Ian Kelly, Security and Trust Engineer, Google *(presentation will not be posted)*

Keynote:

Linda Y. Cureton is the Chief Executive Officer and Founder of Muse Technologies, Inc. The Former NASA CIO, Ms. Cureton launched her new company in April 2013. Muse Technologies, Inc. will provide IT-Enabled Leadership, strategic planning, program management and information technology consulting to both private and government sector organizations. Ms. Cureton attended Washington, DC public schools and was in the very first graduating class of Duke Ellington School of the Arts in 1977. In 1980, she graduated from Howard University with a BS in Mathematics. She later received a Master of Science degree and post-Masters advanced certificate in Applied Mathematics at Johns Hopkins University. Linda is well known as a strong leader and innovator. While CIO, she created the popular NASA CIO blog and continues to be a prolific blogger. She received significant recognition for being a pathfinder for other federal CIOs in professional use of social media.

New Approaches to Security in a Web-Based World

With the rapid adoption of mobile devices and cloud computing in people's personal lives, the demand for access to these technologies in the workplace have accelerated. Are these new technologies incongruous with a secure approach to managing data?

Get a closer look at Google's approach to security from the datacenter to the laptop, the browser and the mobile device. Specifically this talk will focus on providing security at scale, the conundrum of security versus usability and how Google seeks to keep users safe without imposing stringent requirements on how and where they use Google systems.

Ian Kelly, Security and Trust Engineer, Google. Ian is a graduate of Amherst College with a double major in Computer Science and Economics. His career has wandered from consulting to project management, and from startup companies to Google. He has run large technical teams, guest lectured to postgraduate classes and generally has a hard time explaining a "typical day" in his life. But, if given a few minutes Ian will doubtless start talking about some aspect of big data, mobility, security or, more likely, how they all intersect and overlap.

10:20 – 10:35 am (time extended if needed)	**Pecha Kucha (Lightning Round)** Moderator: TBD **Perspective** - Sandra Toner, ICF Jacob & Sundstrom
10:35 – 10:45	Morning Networking Break – hallway outside Green Auditorium

Portrait Room (located across from cafeteria)	Government Best Practice Poster and Demonstration Session
10:35 – 11:00 Will remain open until 1:15 – also visit during lunch	• **Department of Education's FY14 Cyber Security and Privacy Awareness Course** Deborah Coleman, ED and Karen Urban, K2Share • **DHS National Initiative for Cybersecurity Careers and Studies (NICCS): The One-Stop-Shop for Cybersecurity Careers and Studies** Shannon Nguyen, DHS *http://niccs.us-cert.gov/* • **Department of State - Cybersecurity Awareness Team** Alexis Benjamin, DoS • **DoS Cybersecurity On-Line Learning (COL) Program** Mike Riley, Caren Sax, Don Vanderau, DoS • **FISSEA Security Contest Entries** Contest Coordinator: Gretchen Morris, DB Consulting/NASA
11:00 – 11:55 am	**Perspective from Our Educators of the Year Panel** Panel Coordinator: Susan Hansche, Avaya Gov Solutions Including George Bieber, Louis Numkin, Brenda Oldfield, K Rudolph, Jim Wiggins, and others

Government Best Practice Poster and Demonstration Session – Portrait Room

Department of Education's FY14 Cyber Security and Privacy Awareness Course

The Department of Education's will showcase their products including their posters, newsletters and FY14 Cyber Security and Privacy Awareness course.

Department of Homeland Security National Initiative for Cybersecurity Careers and Studies (NICCS): The One Stop Shop for Cybersecurity Careers and Studies

To help ensure a secure cyberspace, we as a nation must develop a technologically-skilled workforce, a cyber-savvy public, and an effective pipeline of future employees. The U.S. is making a substantial investment in developing the workforce of cybersecurity professionals and informing the public about how to manage personal safety online.

The National Initiative for Cybersecurity Careers and Studies (NICCS) is a key resource of cybersecurity information. NICCS directly supports the three components of The National Initiative for Cybersecurity Education (NICE) that focus on enhancing awareness, expanding the pipeline and evolving the field. NICCS is a national resource available to anyone from government, industry, academia, and the general public who seeks to learn more about cybersecurity and opportunities in the field.

Department of State - Cybersecurity Awareness Team

The Department of State Office of Computer Security will demonstrate the breadth of its cybersecurity awareness program, to include elements such as digital communications, traditional and social media, events, and some of the latest hot topics and trends. Stop by to learn about the program's various products and initiatives designed to increase user awareness.

FISSEA Security Contest Entries

Gretchen Morris, Coordinator, of the FISSEA contest will share all contest entries. Submissions showcase one or all of the following awareness, training, and/or education items that are used as a part of your Security program.
Categories:

- Awareness Poster
- Motivational Item (aka: trinkets - pens, stress relief items, t-shirts. etc.)
- Awareness Website
- Awareness Newsletter
- Role-Based Training & Education: Note that this category is for "Role-Based" training and will exclude the "user" role.

“Perspective from our Educators of the Year”

Another first for FISSEA! Join us for this panel discussion with our Educator of the Year (EOY) recipients and hear their perspective on the state of cybersecurity awareness, training, and education. We have invited our EOYs - those influential leaders who have demonstrated a superior level of expertise, effectiveness, and dedication to the advancement of the information system security awareness, training, and education profession – to join us for the session. This is an open Q&A session where we will ask our EOY panel to talk about their best and worst ideas for improving cybersecurity programs and we want our audience members to participate in the interactive discussion by asking their own questions.

11:55 – 1:15 pm	**Lunch Break – NIST Cafeteria Rear** **NIST Tour – sign up at registration desk, two 45-min walking tours** **Final Chance to Visit the Government Best Practice Poster and Demonstration Session in the Portrait Room**
	Green Auditorium
1:15 – 2:00 pm	**Garbo, D-day and Ultimate Social Engineering** **John O’Leary, CISSP, President, O’Leary Management Education**
2:05 pm	**Door Prize Drawing – Green Auditorium and Conference Close**

Garbo, D-day and Ultimate Social Engineering

Social Engineers in 2014 can be clever, creative and trust-inducing as they go about their (usually) nefarious deeds. But not one of them has or will come close to the exploits of an unassuming Spanish chicken farmer who convinced the Germans that D-Day’s primary target was not Normandy. The web of deception that Juan Pujol and a few others wove kept overwhelming forces away from the invasion beaches long enough to ensure that the largest and most complex invasion ever attempted would not be pushed back into the sea. From this convoluted story we can learn some valuable lessons regarding social engineering - perpetrators, targets, methods, obstacles, dangers and consequences, both intended and unintended.

John G. O'Leary, CISSP, is President of O’Leary Management Education. A computer security practitioner since 1977, he has designed, implemented, maintained, administered, broken, troubleshot, fixed, re-fixed, managed, consulted on and taught security for networks ranging from single-site to multi-national. John has been participating in FISSEA since before it was called FISSEA. Recipient of the 2004 COSAC award, the EuroSec 2006 Prix de Fidelite and the 2011 ISC2 Lifetime Achievement Award, his background spans programming, systems analysis, auditing, project management, operations and quality assurance.

Unlike “Garbo,” John has rarely, if ever, been able to fool anybody about anything. This eliminates him for consideration in the spying game, but has gotten him into all sorts of other trouble.

Thank you…..

- **Attendees. We hope you found our conference of value.**
- **Speakers for donating their time, energy, and knowledge.**
- The Technical Working Group for input on the agenda, following-up with speakers, coordinating contests, assisting with the on-site details, and adding new ideas to the program.
- NIST Computer Security Division support: Kevin Stine, Pat Toth, Peggy Himes. Judy Barnard for designing the Program cover and FISSEA website maintenance. http://csrc.nist.gov/fissea
- NIST Conference Office: Mary Lou Norris, Teresa Vicente, Gladys Arrisueno, and AV technicians.
- Federal Business Council (FBC): Shannon Grady Lee and George Hall.