Federal Information Systems Security Educators' Association

fissea

AWARENESS • TRAINING • EDUCATION

29th Annual Conference

March 15-16, 2016

"The Quest for the Unhackable Human: The Power of Cybersecurity Awareness and Training"

fissea

Federal Information Systems Security Educators' Association

AWARENESS • TRAINING • EDUCATION

29th Annual Conference

"The Quest for the Un-hackable Human: The Power of Cybersecurity Awareness and Training"

National Institute of Standards and Technology

Gaithersburg, Maryland

Tuesday, March 15, 2016	AGENDA as of March 8, 2016	
8:00 – 8:55 am	**Registration, Breakfast Snack, and Networking - Hallway outside Green Auditorium**	
9:00 – 9:15 am Green Auditorium	**Conference Welcome –** Patricia Toth, NIST, Conference Chair **NIST Welcome –** Dr. Charles H. Romine, Director, Information Technology Laboratory	
9:20 – 9:50 am Green Auditorium	**Keynote: R U #Unhackable?** Reuben Abishai Paul, Founder/CEO, CyberShaolin & Prudent Games	
9:55 – 10:35 am Green Auditorium	**Privacy and Social Media** Dr. Lisa Singh, Georgetown University	
10:40 – 10:55 am	**Morning Networking Break - Hallway outside Green Auditorium**	
	Track 1: Green Auditorium MC: Pat Toth	**Track 2: Lecture Room A MC: Louis Numkin**
11:00 – 11:30 am	**Digestible Bites of Cyber Security Awareness – Security Bytes, a Case Study** Cheryl Seaman and Stephanie Erickson, NIH	**Mobile Device Security and the Internet of Things** Dr. Karen Paullet, American Public University
11:35 am – 12:05 pm	**Meaningful Training? Federal or a Private Sector approach?** Dr. Luis O. Noguerol, ADITusa/ NOAA Fisheries	**Mobile Device Security** Terry Clapp, DOS/EdgeSource, Inc.
12:05 – 1:00 pm	**Lunch – NIST Cafeteria Rear** **West Square Speaker: WTF: What the Format!!!** Sandra Toner, ICF International	
Prize Drawing 1:05 – 1:35pm Green Auditorium	**Presentation of FISSEA Security Contest Winners** by Gretchen Morris, Contest Coordinator **2015 FISSEA Educator of the Year Presentation**	
1:40 – 2:10 pm	**AppSec Awareness: A Blue Print for Security Culture Change** Chris Romeo, Security Journey	**Conflict Changing Curriculum** Dr. Loyce Pailen, UMUC & Bruce deGrazia, UMUC
2:15 – 2:45 pm	**If we build it, will they come? *Starting the DHS CDM Awareness and Training Program*** Susan Hansche, DHS	**Adding Emotion to Training: *Turning "trainees" into "recruits" by adding emotion to training*** Perry Borenstein, Independent Researcher
2:45 – 3:00 pm	**Afternoon Networking Break/Snack - hallway near Green Auditorium**	
3:05 – 3:55 pm Panel	**Building effective cyber resilience: investing in awareness and behavior change** Nick Wilding, AXELOS Global Best Practice & Rhonda MacLean, MacLean Risk Partners	**Prove it! Gaining Confidence Through Effective Cyber Security Training** Jeff Arsenault and Noah Powers, Delta Risk LLC
4:00 – 4:30 pm	**Cybersecurity Shorts: Short Cyber Training Videos for Today's Workforce** Dr. Kelly Wright, Department of Veterans Affairs	**Attack Surface Reduction: A New Paradigm in Security Awareness with Techniques to Reduce Vulnerabilities and Fight Attacks** Kathleen Fishman, Netorian, LLC
4:35 – 5:15 pm	**IG Metrics: Maturity Model and the New IG FISMA Assessment Approach** John Ippolito, Independent Consultant & Mary Harmison, Federal Trade Commission	
5:20 Prize Drawing	**Dinner Get Together – Location Quincy's (Dinner is not included in reg fee. Sign up at conference.)**	

fissea

Federal Information Systems Security Educators' Association

AWARENESS • TRAINING • EDUCATION

29th Annual Conference

"The Quest for the Un-hackable Human: The Power of Cybersecurity Awareness and Training"

National Institute of Standards and Technology

Gaithersburg, Maryland

Wednesday, March 16, 2016 AGENDA as of March 8, 2016

8:00 – 8:50 am	**Registration, Breakfast Snack, and Networking - Hallway outside Green Auditorium**	
8:50 – 9:05 am Green Auditorium	**Welcome Day 2 Morning Announcements:** Pat Toth, NIST **Vendor and Federal Agency Exhibition Preview Slide Show**	
9:10 – 9:40 am Green Auditorium	**Keynote: Raising Cybersecurity Awareness at a Small Agency, What Works for Me*, Will it Work for You*** Ralph Mosios, CISO, Federal Housing Finance Agency (FHFA)	
9:45 – 10:05 am	**Pecha Kucha (Lightning Round) and Speak-Out (option to sign up on-site)** Moderator: Art Chantker, Potomac Forum, Ltd **Building the 'Force: Disney's Star Wars Insight on the Cyber Work Force,** Sandra Toner, ICF **Fun with Security Awareness**, K Rudolph, Native Intelligence and Niomi Rosenberg, Nomi Designs **Smart City Architecture and Security - A Case Study in Cybersecurity Education**, Paul Wang, UMBC	
Visit the Vendor and Federal Agency Exhibition Poster Hallway Open 10:00 2:45 pm		
10:10 – 10:40 am	**Morning Break – Visit Vendor and Federal Agency Exhibition in Poster Hallway** **View the FISSEA Security Contest entries in the Cafeteria West Square**	
	Track 1: Green Auditorium MC: Pat Toth	**Track 2: Lecture Room A MC: Louis Numkin**
10:40 – 11:10 am	**Gamified Information Security Training: Did it work for a Government of Canada Department?** Jane Moser, Employment and Social Development Canada and John Findlay, Launchfire	**We Have Met the Enemy: Keys for Preventing Insider Threat In Your Organization** Albert Lewis, Federal Housing Finance Agency (FHFA)
11:15 – 11:45 am	**Awareness: An Anti-virus Program for Humans** Gretchen Morris, DB Consulting Group, Inc.	**General deterrence theory, the individual, and what the cybersecurity person needs to know** Charles Wade, DSD Labs
11:50 – 1:10 pm	**Lunch – NIST Cafeteria Rear** **Visit the Vendor and Federal Agency Exhibits in the Poster Hallway**	
1:15 – 1:45 pm	**The Challenge of Creating an Adaptive Awareness Program** Tom Pendergast, Ph.D., MediaPro	**Social Networks: Unsafe at Any Speed?** Carl Willis-Ford, CSRA, Inc.
1:50 – 2:20 pm	**The missing link in your security awareness program…. Internet Tradecraft!!** Russ Haynal, Information Navigators	**Information Assurance for Executives & System Owners** Michael Petock, DOS
2:25 – 2:45 pm	**Afternoon Networking Break/Snacks – Last chance to visit Vendors in Poster Hallway**	
2:45 – 3:30 pm Panel	**The un-hackable human myth: Transforming goals of cyber education to reflect the reality of future threats** Dan Waddell, (ISC)2; Dr. Robert (Rocky) Young, MITRE; Christina L. Phibbs, MITRE; Peter Gouldmann, U.S. Department of State	
3:35 – 4:05 pm	**Awareness to Action: Advancing Human Defense** Ellen Powers, The MITRE Corporation	**Cyber Ethics** Craig Holcomb, NSA (Retired)
4:10 – 4:50 pm	**Unbundling Cyber Security: Integrating Cyber Security Awareness in the Community** Dr. Edna Reid, James Madison University (JMU)	
4:55 pm	**Conference Close - Green Auditorium – Prize Drawing**	

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

29th Annual Conference
"The Quest for the Un-hackable Human: The Power of Cybersecurity Awareness and Training"
National Institute of Standards and Technology
Gaithersburg, Maryland

2016 CONFERENCE PROGRAM

Presentations (with permission) will be posted on http://csrc.nist.gov/fissea
The Program is in order of appearance in the agenda.
Feel free to attend sessions in either room; no need to pre-select.

Tuesday, March 16, 2016

Conference Welcome – Patricia Toth, NIST, FISSEA Conference Chair

Pat Toth is a Supervisory Computer Scientist in the Applied Cybersecurity Division at NIST. Her current project areas include information security, cybersecurity awareness, training and education. Pat is the lead for the Small Business Outreach, Chair of the FISSEA Technical Working Group, Chair of the Federal Computer Security Program Managers' Forum 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 to the National Security Agency.

NIST Welcome – Dr. Charles H. Romine, Director, Information Technology Lab

Charles Romine is Director of the Information Technology Laboratory (ITL). Dr. Romine oversees a research program designed to promote U.S. innovation and industrial competitiveness by developing and disseminating standards, measurements, and testing for interoperability, security, usability, and reliability of information systems, including cybersecurity standards and guidelines for Federal agencies and U.S. industry, supporting these and measurement science at NIST through fundamental and applied research in computer science, mathematics, and statistics. Through its efforts, ITL supports NIST's mission to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.

Within NIST's traditional role as the overseer of the National Measurement System, ITL is conducting research addressing measurement challenges in information technology as well as issues of information and software quality, integrity, and usability. ITL is also charged with leading the nation in using existing and emerging IT to help meet national priorities, including developing cybersecurity standards, guidelines, and associated methods and techniques, cloud computing, electronic voting, smart grid, homeland security applications, and health information technology. Education: Ph.D. in Applied Mathematics and B.A. in Mathematics from the University of Virginia.

Keynote: R U #Unhackable?

Reuben Abishai Paul, Founder/CEO, CyberShaolin & Prudent Games

Strong passwords, Firewalls, Encryption, Anti-malware are examples of some techniques and technologies that can make you secure, but can they make you unhackable?

In this keynote, 10 year old Reuben Paul aka "RAPst4r" will cover and demonstrate "What really makes one Unhackable?"

Come for a fun-filled interactive presentation and find out if you are unhackable?

Reuben Paul is 10 years old kid attending Harmony School of Science in Austin, TX. He lives a life on the edge, between his school, as a straight 'A' student and all of his other passions. When he is not playing video games or on the computer, he likes to read, and takes classes to play inline Hockey, Swim, do Gymnastics, Shaolin Do KungFu, play Piano, Drums and do Art. Reuben is an invited speaker, delivering awareness talks and keynotes on the importance of teaching CyberSecurity to kids and adults. He has been featured at several industry leading Information Security conferences such as RSA, DerbyCon, (ISC)2 Security Congress, Houston Security Conference, Ground Zero InfoSec Summit (New Delhi), BSides Austin, Hack In The Box (HITB) HaxPo conference (Amsterdam) and the Kaspersky Security Analyst Summit (Tenerife, Spain).

When kids from all over the world started to write to him, expressing an interested to learn from him, with the help of his parents, Reuben founded a non-profit cybersecurity awareness and education organization called CyberShaolin which has the mission to educate, equip and empower kids with cybersecurity knowledge, using videos and games that he is developing. He also founded and serves as CEO of Prudent Games Inc, a company that serves to educate while entertaining his customers with the motto, "Learn While You Play".

Reuben was honored to become the youngest person to have received the Shaolin Do Kung Fu Black Belt in America (August 22, 2013) and is now a 2nd degree black belt (earned August 26, 2015). He was the gold medalist in the 2014 USA Gymnastics State competition for the 'rings' category. When he was two years old, Reuben was also crowned as America's Most Beautiful Baby by New Star Discovery. Reuben's twitter handle is @RAPst4r and he has1400+ followers. He has also been painted by the artist Eddie Mize for his contributions to the world of cybersecurity.

Privacy and Social Media

Dr. Lisa Singh, Graduate Director, Associate Professor, Department of Computer Science, Georgetown University

With the growth of online social networks and social media sites, the increase in dynamic web content, and the popularity of digital communication, more and more public information about individuals is available on the Internet. This talk will begin by discussing different ways personal information is exposed on the web. I will then describe different methods that adversaries use to piece together a person's profile and generate 'web footprints'. Using different adversarial attacks, I will show how to quantify a user's level of information exposure relative to others with similar traits, as well as with regard to others in the population. Finally, the talk will conclude with a discussion about strategies we would deploy to educate people about data privacy and ethical uses of public data.

Dr. Lisa Singh is the Graduate Director and an Associate Professor in the Department of Computer Science at Georgetown University. Her research interests are in data science, data mining, and databases. Dr. Singh has authored or co-authored over 50 peer reviewed publications and 5 book chapters. Her research has been supported by the National Science Foundation, the Office of Naval Research, the Social Science and Humanities Research Council, and the Department of Defense. She currently has funding to study privacy on the web (adversarial inference), dolphin social structures with the Shark Bay Dolphin Research project (graph databases, visual analytics and social mining) and forced migration with the Institute for the Study of International Migration, LLNL, York University and others (text mining, graph mining, event detection). Dr. Singh has also been involved with organizing multiple workshops involving future directions of big data research. Dr. Singh received her B.S.E. degree from Duke University and her M.S. and Ph.D. degrees from Northwestern University. She has served on many organizing and program committees, including KDD, ICDM, ICDE, and SIGMOD, and is currently involved in different organizations related to women in computing and computational thinking education for K-12.

Two tracks start at 11:00. Green Auditorium and Lecture Room A – Agenda lists room location

Digestible Bites of Cyber Security Awareness – Security Bytes, a Case Study

Cheryl Seaman, Policy and Awareness Team Lead, and Stephanie Erickson, Training Developer/Instructional Designer, The National Institutes of Health (NIH)

Although cybersecurity awareness has always been a hard sell, the National Institutes of Health (NIH) has developed a multifaceted approach to delivering information that is having increasing success and popularity in our agency. We call them "Security Bytes" with a tagline of "Understanding information security one bite at a time!" Meant to be "edutaining" resources geared at both educating and entertaining the end user, Security Bytes are branded (with a dog that has a human smile), distributed via email, link to a 2-3 minute in-house developed video, and state basic facts about one subject. They are short, colorful, easy to understand, and engaging. They include a question and answer section relevant to the recipients, and one "Did you know?" section. A colorful and branded poster that security officers can post also matches each Security Byte. The idea is to have multiple means of presenting the information. NIH will present a case study of why we decided on this approach, as well as the challenges, successes, and evaluative efforts we have met and pursued in our quest to create more "un-hackable humans". Other organizations may be interested in using this type of awareness strategy and we will share the resources we have developed, including previous Security Bytes, videos, and posters.

Cheryl Ann Seaman, M.P.H., is the Team Lead for Policy, Awareness and Training within the NIH Information Security Program, National Institutes of Health. She is a retired Captain of the US Public Health Service. Originally a Nurse Officer, Cheryl has worked in the Clinical Center, a variety of research administrative positions within the NIH, (including both intramural, extramural programs), served as the NIH Privacy Act Officer, and has been with the Information Security Program since 1998. Her philosophy for creating training is to make it as interesting or *edutaining* as possible.

Stephanie Erickson is a training developer at the National Institutes of Health (NIH) from Triumph Enterprises. She received her B.S. in neuroscience from Brigham Young University. Her previous positions have included teaching assistant for the college of nursing study abroad program at BYU, and e-learning coordinator at the National Science Teachers Association. The author of the *Security Bytes*, Stephanie enjoys bringing entertaining and educational information security materials to the NIH audience. She also helps develop information security training courses. When not knee-deep creating the next *Security Bytes* video or training course, Stephanie can be found playing the piano, working on her next sewing project, or serving with the youth group she leads. She and her husband live in Maryland.

Mobile Device Security and the Internet of Things

Dr. Karen Paullet, American Public University

As of 2016, there are more mobile devices in the world than there are people. Mobile devices have become ubiquitous within our society, and many would now consider them a necessity rather than a convenience. The Internet of Things (IoT), which has been the subject of industry analysts, is the concept of connecting any device with the ability to transfer data over a network. Industry, government and the private sector need to address the security implications of connecting mobile devices. What are the biggest risks associated with the IoT? What are the benefits of the IoT to an organization? How will organizations keep information safe?

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.

Meaningful Training? Federal or a Private Sector approach?

Dr. Luis O. Noguerol, President & CEO, Advanced Division of Informatics and Technology (ADIT) USA/ NOAA Fisheries

Recently OPM security breaches clearly denote that even when multiple efforts have been made to enforce Federal Standards, insufficient training has been leading not only to this, but other security incidents as well. Cybersecurity training at Federal Government level appears as a “very formal” requirement, that based on recent statistics and security incidents are not working as expected or foreseen. Are the controls suggested by NIST working as estimated? Are federal employees familiar with current security threats and what they can do to minimize the risks of data corruption, data exposure and the prospect of leakage of all types of data and information? Is a one year-time mandatory training sufficient to keep employees and contractors engaged? How about motivation? Are “facilities” provided to IT personnel sufficient to keep them aware of current issues? Is theoretical training combined with real-life experience situations and if so, is the process working? Are required IT certifications relevant anymore for cybersecurity roles?

Dr. Luis O. Noguerol, founder, President & CEO of Advanced Division of Informatics and Technology, Inc. has over 31 years of experience in the field of informatics, electronics, telecommunications, and electronic data security. Has a Doctoral degree in Information Technology with concentration in Information Security, a Master Degree in Mathematics, and a second Master Degree in Telecommunications; possesses 32 of the most relevant information technologies certifications recognized by the industry, as for example Certified Ethical Hacker v3 & v8; Computer Hacking Forensics Investigator v3 & v8; ITIL v.3; Check-Point Certified Security Master (CCSM); Certified Internet Web Security Enterprise Administrator (CIW); Qualified Internal Auditor (QIA); ProofPoint Enterprise Protection/Privacy Accredited Engineer (EPPAE); Microsoft Certified Solutions Expert: Server Infrastructure 2012 (MCSE 2012); Certified Business Architect (CBA); IASSC Certified Lean Six Sigma Black Belt (ICBB), and Cisco CCNP Security among many others. Also, Dr. Noguerol has been CISSP certified/re-certified from 2008-2014; has a Bachelor Degree in Aviation Radars Engineering, a second Bachelor Degree in Networking and Telecommunications, in addition to an Associate Degree in Operation and Programming of Management Consoles. Dr. Luis O. Noguerol is also a TTA and Global Knowledge verified IT/Security training professional and have been delivering classes for Bachelor and Master Programs for different Colleges and Universities. At the present moment, Dr. Noguerol work as well as a Part-Time IT/Security Instructor for New Horizons South Florida where was selected as Instructor of the Year (2015), and one of the "Top 10 New Horizons Technical Instructor of the world."

Mobile Device Security

Terry Clapp, Senior Information Assurance Instructor, US Department of State, Information Assurance Branch (EdgeSource, Inc.)

This presentation addresses smart phone technology and its vulnerabilities such as malware, phishing, GPS information and remote tracking, camera functions, encryption and system monitoring. Also discussed will be security measures for mitigation of these vulnerabilities and common practices for enhance personal security.

Terry Clapp served 17 years of active duty with the Air Force and taught higher education for more than 20 years. After September 2001, Terry returned to the Department of Defense as a contractor performing Information Assurance Certification and Accreditation assessments for Tricare Management Activity for 10 years. He recently joined the State Department at the Diplomatic Security Training Center (DSTC) to teach courses in Information Assurance.

Lunch – 12:05 – 1:00 pm

- For those that registered with catering: Food will be served in the back of the cafeteria. Sit anywhere you would like.
- For those that registered without catering: You can go through the cafeteria line, pay on your own, sit anywhere. You can go off campus to a restaurant and return through any gate showing your Conference Badge and photo ID.
- Lunch Speaker Option – There will be a lunch speaker in the West Square. After you get your lunch, you can eat in the West Square (located near the back of the cafeteria) and listen to our lunch speaker. Seating is limited.

Lunch Speaker: WTF: What the Format!!!

Sandra Toner, Technical Specialist, ICF International

WTF: What the Format!!! Cyber Risk Management doesn't have to be taught on a computer. Using a few interactive games, Mrs. Toner will illustrate how engaging traditional delivery formats can illuminate fundamental security concepts. Participants will be encouraged to try a demonstration of art and reading, music, and tactile games teach secure computing fundamentals without the most common delivery mechanism- a computer.

Sandra Toner is a Certified Technical Trainer (CompTIA CTT+) who teaches about software, cyber security, and information assurance. She is a Cyber Risk Management nerd. She holds a Project Management Professional (PMP) certification as well as a graduate certificate in Open-source Intelligence Analysis. Since 2000, she has taught in post-secondary education, facilitated computer security and compliance training for the federal government, and provided training for technical platforms and proprietary software. She is a member of a number of security and cyber risk related professional communities and likes to be involved at the ground level by participating in government and industry working groups.

Prize Drawing 1:05 – 1:35 pm Green Auditorium	**Presentation of FISSEA Security Contest Winners** **by Gretchen Morris, Contest Coordinator** **2015 FISSEA Educator of the Year Presentation**

FISSEA Security Awareness, Training, and Education Contest

Entrants were asked to showcase one or all of the following awareness, training, and/or education items that are used as a part of their Security program. Categories: (1) Awareness Poster; (2) Motivational Item (aka: trinkets - pens, stress relief items, t-shirts. etc.); (3) Awareness Website; (4) Awareness Newsletter; (5) Awareness Video; (6) Role-Based Training & Education: Note that this category is for "Role-Based" training and will exclude the “user” role. Please limit your entry to the coverage of one skill within a role-based training or education course. Gretchen Morris coordinates this contest and enlists an impartial judging committee.

Winning entries are announced at the annual conference and receive a framed certificate along with bragging rights.
See winning items on http://csrc.nist.gov/organizations/fissea/FISSEA-contest/previous-winners.shtml

2015 FISSEA Security Awareness, Training, and Education Contest

Awarded Certificates at Conference (selected by impartial judging committee prior to conference):
Poster Winner: Kelly Wright – VA IT Workforce Development
Website Winner: NASA IT Security Awareness and Training Center
Motivational Item Winner: Jane Moser – Employment and Social Development Canada (ESDC)
Newsletter Winner: Wendy Andrews, Robert Collins, Arnold Ginn, and CDR Steven Miller – Indian Health Service
Role-Based Training Winner: Jane Moser – Employment and Social Development Canada (ESDC)

Peer’s Choice Awards (selected by peers during the conference):
Poster Winner: Kimberly Conway, Sara Fitzgerald, Sean Hanion, Dave Stapleton, and Steven VanBrackle, FDA
Website Winner: Kimberly Conway, Sara Fitzgerald, Sean Hanion, Dave Stapleton, and Steven VanBrackle, FDA
Motivational Item Winner: Cindy Dailey, Geisinger Health System
Newsletter Winner: Brenda L. Ellis, NASA
Role-Based Training Winner: Jennifer Young, Communication Security Establishment

2016 Winning entries will be posted to FISSEA website

FISSEA Educator of the Year Award

The FISSEA Educator of the Year Award was established to recognize and honor a contemporary who is making special efforts to create, build, manage, or inspire an information systems security awareness, training, or education program. Sam Maroon presented the FISSEA 2014 Educator of the Year posthumously to Shon Harris of Logical Security. Mr. Maroon shared Ms. Harris’ contributions to the cyber security education industry by characterizing her contributions in three ways, as a writer, a trainer, and a thought leader. Ms. Harris’ friends and colleagues, Michael Lester and Hamid Dehghan accepted the plaque on her behalf.

Surprise – the 2015 Educator of the Year is announced at the March 2016 Conference.

Nomination information see http://csrc.nist.gov/organizations/fissea/educator-year/recipients.shtml

2014
FISSEA Educator
of the Year
Presented
Posthumously
to

Shon
Harris

on March 24, 2015

Accepting the award were Michael Lester and Hamid Dehghan with Sam Maroon.

FISSEA Educator of the Year Award RECIPIENTS:

2015: Surprise – announcement made March 15, 2016
2014: Shon Harris, Posthumously, Logical Security
2013: Sam Maroon, FITSI Foundation / Wounded Warrior Cyber Combat Academy
2012: J. Paul Wahnish, Career Technical Education Foundation, Inc.
2011: Susan Hansche, Avaya Government Solutions
2010: Jim Wiggins, Federal IT Security Institute
2009: Brenda Oldfield, Department of Homeland Security
2008: Luke Andersen, Global Knowledge
2007: David Kurtz, Treasury, Bureau of the Public Debt
2006: COL. Curtis Carver, United States Military Academy
2005: K Rudolph, Native Intelligence, Inc.
2004: Dr. Gail-Joon Ahn, University of North Carolina
2003: Jeff Recor, Walsh College
2002: Patricia Black, United States Department of Treasury
2001: LTC Daniel Ragsdale, United States Military Academy
2000: George Bieber, Defense Information Systems Agency (DISA)
1999: Dr. Roger Quane, National Security Agency
1998: Louis Numkin, Nuclear Regulatory Commission
1997: Dorothea de Zafra, National Institute of Health
John B. Ippolito, Allied Technology Group, Inc.
Sadie Pitcher, U.S. Department of Commerce
John Tressler, U.S. Department of Education
1996: Joan Pohly, Defense: Defense Information Systems Agency
1995: Gale Warshawsky, Department of Energy: Livermore Nat Lab
1994: Lt. Col. E. C. "Lee" Chambers, U.S. Air Force
1993: Dr. Corey Schou, Idaho State University
1992: Dr. Vic Maconachy, National Security Agency
1991: Dr. Gary W. Smith, Department of Defense

Two tracks again – 4:35 back to one presentation – prize drawing at end of day

AppSec Awareness: A Blue Print for Security Culture Change

Chris Romeo, CISSP, CSSLP, CEO, Security Journey

How does an individual change the application security culture of an organization? By designing and deploying an application security awareness program that contains engaging content, humor, and recognition. Application security awareness is part security knowledge, part lessons learned from history, and action to improve security. Each organization has an application security culture, but most of them are lacking.

This session is about exposing each audience member to a successful blue print for how they can build an application security awareness program of their own. The content is based on real life experience implementing application security awareness in a large enterprise reaching 30,000 people. Go beyond traditional security awareness, and dive deep into changing the DNA of those who code, test, and manage applications within their company.

In our reference example the content ranges from introductory to advanced, using belts to measure achievement and provide recognition. As students progress, they migrate from knowledge acquisition into actions to improve security. A system of tracking and recognizing achievement-based activities gets people fired up to make security improvements. The reference example exists as the backdrop, but the emphasis is focused on the blue print for the audience to create such a program themselves.

Chris Romeo is CEO, Principal Consultant, and co-founder of Security Journey. His passion is to bring application security awareness to all organizations, large and small. He was the Chief Security Advocate at Cisco Systems for five years, where he guided Cisco's Secure Development Life Cycle program, empowering engineers to "build security in" to all products at Cisco. He led the creation of Cisco's internal, end-to-end application security awareness program launched in 2012.

Chris has twenty years of experience in security, holding positions across the gamut, including application security, penetration testing, and incident response. Chris is a sought after conference speaker, with experience speaking at the RSA Conference, ISC2 Security Congress, AppSec USA, and many others.

Conflict Changing Curriculum

Dr. Loyce Best Pailen, CISSP, Collegiate Professor, Graduate School of Management and Technology, University of Maryland University College (UMUC) & Bruce deGrazia, JD, CISSP, Program Chair, Cybersecurity Management and Policy, UMUC

UMUC is working on a comprehensive program review/revision for its transformation to competency-based models. UMUC is investing in the capacity to have the best and most compelling programs in the world. To get there, they started the conversation with a clean slate, asking the question "what should students know and be able to do when they graduate from the best program in the world in my area?" This freed the university to think outside of the boundaries of what we currently do, and literally "whiteboard" the best cybersecurity and information assurance programs in the world. The university looked to the professional organizations and/or accrediting bodies for input into their programs and received overwhelming guidance about what students should know and be able to do upon graduation. As well, the university took a glance at a few aspirant schools to see what they had and most importantly, using its cadre of scholar practitioners identified the competencies that are critically important. As such the presentation reviews what the university has done to assemble the fundamental list of all competencies, learning demonstrations and the like, thinking about the cybersecurity profession of today, and tomorrow (i.e., what would students need to know and be able to do 5 years from now in their various cyber professions).

Dr. Loyce Best Pailen, CISSP, has 35+ years of broad experience in information technology including cybersecurity, software development, project management, telecommunications, risk management, and network and systems security and administration. She has held director level positions at The Washington Post, Graham Holdings, University of Maryland University College, and Computer Sciences Corporation contracting for the U.S. Department of Defense, Defense Cyber Investigations Training Academy. Along with her IT experience, Dr. Pailen has provided instructional design and subject matter expertise for the development of major graduate, undergraduate, and community college information systems security curriculum development projects. Among other certifications, credentials, and awards Dr. Pailen is holds the highly recognized CISSP certification. Currently Dr. Pailen is a Full Collegiate Professor within the University of Maryland system teaching Cybersecurity management, policy and technology courses.

Bruce deGrazia, JD, CISSP, is the Program Chair for Cybersecurity Management and Policy at the University of Maryland University College. He comes from Chicago, Illinois, where he graduated from DePaul University with a degree in History. He then took a Master’s degree in Archaeology from the University of London. He returned to DePaul for a degree in International Law. He also has an M.S. in Cybersecurity Technology from UMUC.

Before coming to UMUC, Professor deGrazia worked at the U.S. Environmental Protection Agency, Cummins Engine Company, and United Technologies Corporation. He served in the Navy as an officer in the Judge Advocate General’s Corps and was Assistant Deputy Under Secretary of Defense for Environmental Quality in the Clinton Administration.

Professor deGrazia has spoken on cybersecurity topics worldwide and is Senior Vice President of the National Capital Region Chapter of ISC². He holds numerous IT-related certifications, including the CISSP, and is an Honorary Fellow of Royal Holloway and Bedford New College, University of London.

If we build it, will they come?

Starting the DHS CDM Awareness and Training Program

Susan Hansche, CISSP-ISSEP, Training Manager, Department of Homeland Security (DHS)

Our challenge -- how to provide awareness and training to all federal executive agencies implementing the Department of Homeland Security (DHS) Continuous Diagnostics and Mitigation (CDM) Program. Our learning program identified the audience as geographically dispersed, inconsistent knowledge of the material, mostly non-DHS employees, and at various points of implementation for the multi-phased CDM program. We tried to answer the traditional training requirements during our planning phase to ensure that our solution would have relevance for the majority of our audience – all while using various distribution mediums. In this session, I will briefly discuss our planning process, our solutions, and then will open it to the audience to share your experiences and best practices for creating similar learning programs.

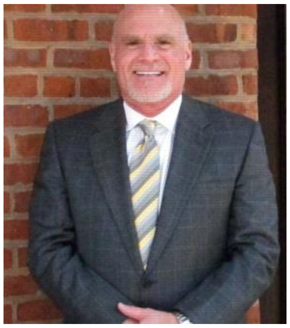
Ms. Susan Hansche, CISSP-ISSEP, has been a FISSEA supporter for many years and is honored to present at the 29th Annual FISSEA Workshop. She is the Training Manager in the Federal Network Resilience office at the Department of Homeland Security. She has over 20 years of experience in the training field and specific expertise in designing, developing, and implementing Information Assurance and Cybersecurity training programs for Federal agencies. For the past 17 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.

Adding Emotion to Training

Turning “trainees” into “recruits” by adding emotion to training

Perry Borenstein, MA Psychology, MEd Education, GISF, GISL, ITIL, Six Sigma, Independent Researcher

As email becomes the preferred method of penetrating networks, criminals, activists, and nation-states are making it more difficult to differentiate the benign from the malicious. To keep up, training must change from informational events to recruiting events so attendees leave with a feeling of responsibility and empowerment to better protect themselves, their families and their employers.



Perry Borenstein spent 30 years developing technology for Wall Street firms, including financial and human resource applications. He also focused on Process Improvement, Incident Management, and Root Cause Analysis. He has an MA in Education from Johns Hopkins, and a Masters in Psychology from The Ferkauf School of Psychology of Yeshiva University. He is currently doing research on Information Security issues.

Building effective cyber resilience: investing in awareness and behavior change

Nick Wilding, Head of Cyber Resilience, AXELOS Global Best Practice & Rhonda MacLean, CEO, MacLean Risk Partners

“Cybersecurity is a serious corporate risk issue affecting virtually all levels of significant business activity. Ultimately, as one director put it: “Cybersecurity is a human issue.” (Cyber Risk Oversight for Boards’, National Association of Corporate Directors, 2015)
Effective cyber resilience is all about people and behaviours, from the boardroom to the frontline. Everyone has a vital part to play in protecting an organizations reputation, customer trust and competitive advantage. People must sit at the heart of an effective cyber resilience strategy. It requires a balanced and collaborative approach across the entire organization – embedding awareness, insight and skills that will make you more effective in keeping your critical information safe.

Sadly many organizations are failing to engage all their people in adopting cyber resilient behaviors. A different approach is required - one that effectively uses the latest learning and communications techniques as well as relevant language for our staff to engage in through new learning and ongoing refresher training.

So how can any organization create appropriate organizational resilience that supports their business strategy through effective staff awareness learning and training?

Nick Wilding, Head of Cyber Resilience, AXELOS Global Best Practice. Nick has spent the last 25 years in senior market development and marketing roles. In his role at AXELOS he leads the Cyber Resilience Best Practice division responsible for the successful design, continued improvement and success of RESILIA - an integrated best practice portfolio designed to help organizations develop effective cyber resilience from the boardroom down. AXELOS is a joint venture between UK Government (Cabinet Office) and Capita plc and owns and develops global best practice including ITIL and Prince2. Before joining AXELOS in March 2014 he spent 11 years at BAE Systems Applied Intelligence where he helped set up their Cyber Security business and led their Cyber Security market engagement, marketing and thought leadership.

Rhonda MacLean, CEO, MacLean Risk Partners, active Board Director and formerly the CISO at Bank of America, Boeing and Barclays. Rhonda’s distinguished career runs the gamut from Chief information Security Officer of Fortune50 companies such as Bank of America and Boeing to international financial services at Barclays plc, to testifying before the US Congress during hearings on cybersecurity. Rhonda has now turned her attention to her private cybersecurity risk management firm and to developing best practices in cyber risk and resiliency for public company boards and managing directors. She serves on the Board of Directors of Red Seal Networks and ThreatMetrix Inc, and on the advisory board of four other organizations. She also serves as Adjunct Distinguished senior fellow with Carnegie Mellon University’s Information Networking Institute (INI).

Prove it! Gaining Confidence through Effective Cyber Security Training

Jeff Arsenault, Director, CISSP and Noah Powers, Senior Associate, CISSP, Delta Risk LLC, A Chertoff Group Company

The quest to conduct effective and meaningful training in Information Security is nearly 20 years in the making, yet the results have come short of producing the required workforce our Nation requires. In 1997 the Government Accountability Office reported the following as factors of IT security as a high-risk area – “poorly designed and implemented security programs,” “shortage of personnel with the technical expertise needed to manage controls,” and “insufficient awareness and understanding of information security risks among senior (agency) officials.” Much the same is often said today in response to increasing cyber attacks and data breaches.

The gap between attacker’s knowledge and our own as defenders is increasing, and not in a good way. To counteract this, the focus must shift from technology to people as the way to gain the upper-hand back from the attackers. We believe an overabundance of security technologies has led to a false sense of security as formal training programs have failed to keep pace. Through trial and error we found the type of training and evaluation process matters as much as the content taught, and the best approaches to effective and meaningful training is through virtual live-fire training events. Security staff understanding the technology at their disposal, and how to use it is key. Combined with an effective evaluation program, organizations can get confident about their security processes and where they need to focus efforts. This talk presents the training and evaluative approaches we have found to be effective.

Jeff Arsenault is a Director with Delta Risk LLC, and has worked in the cyber domain for over 15 years providing cyber exercises, operational Red Team assessments, enterprise vulnerability assessments, and training in defensive and offensive network operations.

Noah Powers is a Senior Consultant with Delta Risk LLC and specializes in cyber exercises focusing on adaptive threat emulation, team communication, and evaluating team and operator effectiveness. Both Jeff and Noah originate from military backgrounds.

Cybersecurity Shorts: Short Cyber Training Videos for Today’s Workforce

Dr. Kelly S. Wright, Instructional Systems Specialist, IT Workforce Development, Department of Veterans Affairs

Think about cybersecurity training produced in a professional studio environment by your internal staff! The Department of Veterans Affairs virtual VA IT Campus Team has created short, bite-sized cybersecurity videos using green screen technology for a professional, polished product. Come see how we have deconstructed one-hour long vendor supplied course materials into “Cybersecurity Shorts” that are no more than 10 minutes in length. These shorts, delivered by CISSPs, provide technical content while engaging the audience with information relevant to their work. You will be introduced to new studio terms and learn how to develop show books that easily organize the recording of a video. Come away with ideas on how to produce videos in your environment and a sample show book to begin developing your own shorts.

Kelly Wright is an Instructional Systems Specialist with IT Workforce Development, for the Office of Information and Technology at the Department of Veterans Affairs. She earned her doctorate in Educational Leadership with a concentration in Educational Technology from Shenandoah University, Winchester, VA in 2005. Working in the academic IT environment, she prepared and earned her Certified Information Systems Security Professional (CISSP) certification in 2009.

Dr. Wright’s work experience includes Lead Associate with Booz, Allen, Hamilton, Chief Information Officer and Instructor for Blue Ridge Community and Technical College, and multiple Adjunct Instructor positions at Shenandoah University (VA) and Shepherd University (WV) teaching Business, Information Technology and Office Technology courses.

Currently, Dr. Wright is developing and presenting a variety of instructional video courses incorporating Micro-learning theory to enhance concept development in what would be considered dry, technical material.

Attack Surface Reduction: A New Paradigm in Security Awareness with Techniques to Reduce Vulnerabilities and Fight Attacks

Kathleen Fishman, CISSP, CEH, CCNA, Netorian LLC

This presentation includes a LIVE CYBER-ATTACK DEMONSTRATION with a step-by-step implementation of defensive countermeasures. Attendees will learn a strategy and implementation methodology to reduce cyber threats by eliminating targets of vulnerability. As user mode protection tool suites become more prevalent, attackers more frequently utilize advanced attacks such as those against the kernel and memory. Security professionals typically rely upon traditional security tools such as intrusion prevention systems, antivirus, and firewalls combined with a continuous therapy of scanning, patching, and best practices to detect security failures and block future attacks. These tools are failing to keep pace with the growing complexity of cyber threats and provide virtually no mechanism to detect or stop attacks that occur in memory. Reducing the attack surface of operating system activities, application libraries, and network services eliminate vulnerabilities and thereby disable the opportunity for an exploit to occur.

Ms. Fishman is the Cyber Security Architect and Information Assurance Subject Matter Expert for Netorian, LLC. She brings seventeen years of experience in Cybersecurity, Information Assurance, and Cyber Protection Training; holds Bachelor's and Master's degrees in Computer Engineering; and is a Certified Information Systems Security Professional, Certified Ethical Hacker, Cisco Certified Network Associate, and Certified HBSS System Administrator. Ms. Fishman has served as the Technology Lead for Information Security and Information Assurance projects at various Department of Defense organizations including JNCC-A, 106th Signal Brigade, TRADOC, FORSCOM HQ, USAREUR, USARAF, 8th Army, SOF, 1 CAV, 4ID, III corps, 101AD, 10th MTN, 1AD, USF-I, and 25 ID. As an Information Assurance professional, Ms. Fishman has provided Computer Network Defense services for multiple tactical defense systems as well as coalition forces in Afghanistan, Iraq, Kuwait, Germany, Italy, and Korea. Ms. Fishman has provided computer security support and training to various program offices, Warfighting organizations, and the Army Cyber Brigade Team. She was responsible for authoring and instructing cyber security training programs on both basic and advanced features of cyber security and advanced techniques of custom threat detection for the Army Cyber Protection Teams (CPT) and the Office of the Assistant Secretary of the Army for Acquisition, Logistics, and Technology (ASA(ALT)).

IG Metrics: Maturity Model and the New IG FISMA Assessment Approach

John Ippolito, CISSP, PMP, Independent Consultant & Mary Harmison, CPA, Audit Manager, Office of Inspector General, Federal Trade Commission

The Federal Information Modernization Act (FISMA) primarily formalized responsibilities and practices put in place over the last several years through Office of Management and Budget Memorandums. The Act did, however, make a substantial change to the requirement for an annual Inspector General assessment. The 2002 Act required a compliance assessment. The 2014 Act requires an effectiveness assessment. This presentation discusses the potential impact on agency security programs and staff training resulting from this change and the maturity model approach to be used in making this assessment.

Mr. John Ippolito has more than 40 years' experience as an Information Technology (IT) professional, including nine years with the General Accounting Office. He has an extensive technical and management background with special emphasis on cybersecurity and developing secure information systems and system audit techniques. He has more than 14 years' experience conducting annual FISMA security evaluations for CIOs and IGs.

Mr. Ippolito has supported a variety of federal agencies including the DoD Joint Staff; the Departments of Homeland Security, Health and Human Services, Energy, and Education; and the Federal Trade Commission, the Federal Aviation Administration, and the Nuclear Regulatory Commission. Mr. Ippolito was named Federal Information System Security Educator of the Year for 1997.

Ms. Harmison is a licensed CPA with more than 15 years' experience in providing oversight of agency programs and performing independent audits and evaluations of internal and cybersecurity controls. She also develops and conducts federal audit training for the federal community. Ms. Harmison is an adjunct instructor for the Council of Inspectors General on Integrity and Efficiency (CIGIE) Training Institute and has taught in their biannual audit peer review training for February 2012 through August 2015. She is also participating with the CIGIE committee that is developing a maturity model evaluation approach for {what is the work area for the CIGIE committee}.

Ms. Harmison is a certified Contracting Officer's Representative (COR) Level II. Since joining the FTC in 2008, she has provided oversight and quality assessments for both the FTC Federal Information Security Management Act (FISMA) annual evaluations and annual FTC financial statement audits.

Prior to joining the FTC, Ms. Harmison was an auditor with the Library of Congress OIG and conducted audits of federal financial statements as a member of commercial CPA firms. Her experience includes auditing the financial statements of the Library of Congress, James Madison National Council Fund, the Cooperative Acquisitions Program Fund, the National Digital Library Fund, the Government Accountability Office, and the U.S. Senate Restaurants Revolving Fund.

5:20 pm	**Door Prize Drawing – Green Auditorium** **Dinner Get Together – Location Quincy's, Quince Orchard Plaza Shopping Center, 616 Quince Orchard Road, Gaithersburg, MD 301-869-8200** ***(Dinner is not included in the registration fee.)*** **Sign up at conference at the registration desk.**

About NIST (National Institute of Standards and Technology)

Founded in 1901, NIST is a non-regulatory federal agency within the U.S. Department of Commerce. It was known between 1901 and 1988 as the National Bureau of Standards (NBS). NIST's mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life. NIST employs about 3,400 scientists, engineers, technicians, and support and administrative personnel at its headquarters in Gaithersburg, Maryland, and its laboratories in Boulder, Colorado. The agency also hosts about 2,700 associates from academia, industry, and other government agencies, who collaborate with NIST staff and access user facilities.

Dr. Willie E. May is the Under Secretary of Commerce for Standards and Technology and the 15th Director of NIST. NIST has an annual budget of $964 million (2016). The Gaithersburg campus is comprised of 578 acres and the Boulder campus is 208 acres.

Website: http://www.nist.gov.

NIST Computer Security Resource Center (CSRC)

The NIST CSRC is the primary gateway for gaining access to NIST Computer Security publications, standards, and guidelines. http://csrc.nist.gov/ From the Publications page you can access Special Publications (SPs), Federal Information Processing Standards (FIPS) (security standards), Interagency Reports (NISTIRs) (documentation that supports and provides background information for FIPS and SPs), and Information Technology Laboratory (ITL) Bulletins (monthly overviews of NIST's security publications, programs and projects).

SP 800 series**, *Computer Security*** *(December 1990-present)*: NIST's primary mode of publishing computer/cyber/information security **guidelines, recommendations and reference materials**;

SP 1800 series, ***NIST Cybersecurity Practice Guides*** *(2015-present)*: A new subseries created to complement the SP 800s; targets specific cybersecurity challenges in the public and private sectors; **practical, user-friendly guides** to facilitate adoption of standards-based approaches to cybersecurity.

NIST websites of possible interest to FISSEA members:

- NIST CSRC http://csrc.nist.gov/
- FISSEA (Federal Information Systems Security Educators' Association): http://csrc.nist.gov/fissea - March Conference, NIST
- NICE (National Initiative of Cybersecurity Education): http://csrc.nist.gov/nice/ - Nov 1-2, 2016 Conference, Kansas City MO
- NCCoE (National Cybersecurity Center of Excellence): https://nccoe.nist.gov/
- Cybersecurity Framework: http://www.nist.gov/cyberframework/ - April 5-7, 2016 Workshop, NIST
- National Strategy for Trusted Identities in Cyberspace (NSTIC): http://www.nist.gov/nstic/
- FISMA (Federal Information Security Management Act (FISMA) Implementation Project: http://csrc.nist.gov/groups/SMA/fisma/index.html - email alias for FISMA questions sec-cert@nist.gov

Wednesday, March 16, 2016

Green Auditorium	**Morning Announcements: Pat Toth, NIST** **Door Prize Drawing** **Vendor and Federal Agency Exhibition Preview Slide Show** **Poster Hallway – Open 10:00 am – 2:45 pm**

Keynote: Raising Cybersecurity Awareness at a Small Agency, What Works for Me, *Will it Work for You*

Ralph Mosios, Chief Information Security Officer, Federal Housing Finance Agency (FHFA)

Mr. Mosios will discuss some of the security and training initiatives that he implemented over the past five years, including social engineering activities such as spearphishing exercises; how to measure results; and a brief discussion of monthly cyber newsletters. The goal of this program is to make your end users your first line of defense.

Ralph Mosios has over has over 30 years of professional experience in IT security, IT management, software program management, and engineering, supporting both the private and public sectors. Mr. Mosios is currently the chief information security officer for the Federal Housing Finance Agency responsible for network security. Prior to joining the Federal Housing Finance Agency, Mr. Mosios was a senior IT security specialist and acting chief information security officer for the U.S. Securities and Exchange Commission (SEC) for six years. Prior to joining the SEC, Mr. Mosios held numerous consultant IT security and management positions with IBM, PricewaterhouseCoopers, and Booz Allen & Hamilton. Mr. Mosios started his career as an aersopace engineer at the Office of Naval Intelligence and then at the Naval Air Systems Command. Mr. Mosios has an undergraduate degree in aeronautical engineering and a masters degree in engineering managament. Mr. Mosios is a Certified Information Systems Security Professional (CISSP), Certified Ethical Hacker (CEH), and Project Management Professional (PMP).

Pecha Kucha (Lightning Round) and Speak-Out

During Pecha Kucha (Lightning Round) speakers have 6 minutes 40 seconds and the challenge is in limiting one's talk to only 20 slides max, and only 20 seconds per slide. Pecha Kucha (or PK) means "chit chat" in Japanese. It's really challenging to do as a speaker of course, and quite fun for audience members to watch!

Moderator: Art Chantker, President, Potomac Forum, Ltd

- **Building the 'Force: Disney's Star Wars Insight on the Cyber Work Force, Sandra Toner, Sr. Technical Specialist, ICF International**
- **Fun with Security Awareness, K Rudolph, Native Intelligence, Inc. and Niomi Rosenberg, Nomi Designs, LLC**
- **Security in Smart City Architecture - A Case Study in Cybersecurity Education, Paul Wang, UMBC**

Speak-Out

An opportunity for attendees to publicly share their experiences or views on an issue. Sign up at the registration desk.

Art Chantker is the President of Potomac Forum, Ltd., founded in 1982 as a non-profit educational organization, to provide training, seminars, conferences, and other educational events for government. Art has also taught procurement and management of government information technology for over 30 years. Potomac Forum, Ltd. has taught thousands of government and industry executives, managers, and staff at numerous cities throughout the country. Art has chaired numerous conferences, seminars, panels, awards ceremonies and other programs – all focused on the Federal Government. Additionally, Art produced a bi-partisan Inaugural Gala for 1000 government and industry executives and managers.

Art is a retired federal government executive. During his government career he served in several executive leadership positions at the CIO and Director levels at the Departments of Education, Transportation, U.S. Marshals Service and the Office of Naval Research. He also managed two government-wide programs for the National Institute of Standards and Technology where he authored a Federal Information Processing Standard (FIPS) Publication on Computer Selection.

He has been involved in executive leadership positions in numerous professional organizations and associations including twice elected as President of the Association for Federal Information Resources Management (AFFIRM) and is currently a Director. He was a previous Chair of the IAC Software Shared Interest Group and on the Board for Women in Technology. Art serves on the Working Group of the NIST sponsored Federal Information Systems Security Educators' Association (FISSEA) and served on the Board of AFCEA Bethesda Chapter as VP, Government Awards. Art is proud to have served as a Captain in the United States Air Force.

Building the Force: Disney's Star Wars Insight on Team Building

Sandra Toner, Cyber Physical Security Technical Specialist, Project Manager, ICF International

In this Pecha Kucha, Sandy will breakdown a handful of lessons from teams used throughout the Star Wars movies and transfer the concepts into the cybersecurity workforce domain.

Sandra Toner is a Certified Technical Trainer (CompTIA CTT+) who teaches about software, cyber security, and information assurance. She is a Cyber Risk Management nerd. She holds a Project Management Professional (PMP) certification as well as a graduate certificate in Open-source Intelligence Analysis. Since 2000, she has taught in post-secondary education, facilitated computer security and compliance training for the federal government, and provided training for technical platforms and proprietary software. She is a member of a number of security and cyber risk related professional communities and likes to be involved at the ground level by participating in government and industry working groups.

Fun with Security Awareness

K Rudolph, Native Intelligence, Inc. and Niomi Rosenberg, Nomi Designs, LLC

This short talk will share several ideas for boosting the fun in your security awareness program. There will be fabulous prizes, of course.

K Rudolph is the founder and Chief Inspiration Officer of Native Intelligence, Inc., a firm that provides security awareness courses, programs, and materials. K is interested in the psychology of security awareness, learning and behavior, storytelling, and security awareness metrics. She's the author of several books and articles on information security and has been honored as FISSEA's Security Educator of the Year.

Niomi Rosenberg is part of the creative team for Native Intelligence. With a strong background in design and merchandising, Niomi's company, Nomi Designs, LLC has been supporting government contracts for several years.

Smart City Architecture and Security – A Case Study in Cybersecurity Education

Shuangbao (Paul) Wang, Ph.D., Professor, Cybersecurity; Director, Center for Security Studies, University of Maryland, University College (UMUC)

Smart city opens up data with a wealth of information that brings innovation and connects government, industry and citizens. It also improves the livability, workability and sustainability and connects people from urban to suburban areas and gathers data from a large number of Beacons, RFIDs, wearable devices, embedded systems, , and other sensors that are connected through Programmable Logic Controllers (PLCs), Raspberry Pi, Arduino or other microcontrollers. As smart city systems are interconnected, it opens up vulnerabilities.

In this presentation, we look into a case study of smart city architecture and security based on a water treatment system that has more than 3,000 PLCs. The supervisory control and data acquisition (SCADA) system uses the Department of Defense developed technology to collect data. The presenters will also introduce visual mapping in mapping knowledge units to skills in the development of cybersecurity curricula.

Shuangbao (Paul) Wang is a Professor and the Director of the Center for Security Studies at University of Maryland, University College, a National Center for Academic Excellence in Cybersecurity Education designated by NSA and DHS, and a National Center of Digital Forensics by the DoD Cyber Crime Center (DC3).

Paul Wang was previously Chief Information and Technology Officer (CIO/CTO) of National Biomedical Research Foundation (NBRF). He has been consultant to many companies over the years, and serves on multiple boards and government and private sector technology committees. Paul was directly involved in drafting of the National Initiatives of Cybersecurity Education (NICE) framework. His research areas are cybersecurity, smart cities, cryptography and video indexing.

In addition to books, referred publications, conference speakers and numeral grant activities, Paul has four patents; three of them have been licensed to the industry. Paul Wang received his Ph.D. under Dr. Robert Ledley, the inventor of body CT scanner in 2004.

Visit the Vendor and Federal Agency Exhibition in the Poster Hallway   participate in their Bingo game   pick up cards at the registration desk

- ***During the Morning Break 10:10   10:40***
- ***During the Lunch Break 11:50   1:10***
- ***During the Afternoon Break 2:25   2:45***

View the FISSEA Security Contest entries in the West Square near the Cafeteria   vote for Peer s Choice

Gamified Information Security Training - Did it Work for the Government of Canada?

Jane Moser, Security Training and Awareness Program Coordinator, Employment and Social Development Canada
John Findlay, Founder/Program Designer, Launchfire

After a couple of high profile data breaches Employment and Social Development Canada (ESDC) hired Gartner Research to conduct an audit of their security program. One of Gartner's key recommendations was that ESDC needed to invest more in security awareness and training.

To overcome people's aversion to information security training, ESDC engaged Launchfire to develop a game-based learning product which was piloted last fall. The objective was to see if game tactics could make the content more engaging and digestible. So did it work? Now's your chance to find out!

In this session we'll look at how the content was morphed into game-based learning, examining specific gamification tactics that were implemented to amplify engagement, comprehension, and retention. And for the nerds in the crowd, we'll take a look at how the analytics dashboard helped identify knowledge gaps and slackers!

Jane Moser is the Security Training and Awareness Program Coordinator at Employment and Social Development Canada. She and her team develop and deploy security awareness materials in a variety of media including video, print, e-learning, web and now, game-based learning!

Jane also chairs the Interdepartmental Security Awareness Working Group (SAWG) that reports to the Government of Canada Security Council. With approximately 200 members representing over 60 departments, SAWG's mission is to develop and share security awareness materials and best practices which results in resource savings for all. Jane's 28 year career with the federal government began in Saskatchewan and, she now calls Ottawa home.

John Findlay is an expert gamifier. Early on in life John showed promise in the non-existent field of gamification making games out of everything from homework to chopping wood.

While working as an SAP trainer John discovered that by making games out of the training courses he was able to get folks more engaged. This experience inspired john to start Launchfire where he designs game-based, training programs for both public and private sector organizations.

We Have Met the Enemy: Keys for Preventing Insider Threat in Your Organization

Albert Lewis, CISSP-ISSMP, CISM, CGEIT, Federal Housing Finance Agency (FHFA)

Maintaining confidentiality of critical information is essential to government and business operations. Recent highly publicized events involving unauthorized disclosures of classified information by trusted insiders demonstrates the need for better awareness and stronger internal controls. This session discusses the key indicators of an insider threat and the importance of security education, training, and awareness to stopping insider threat. Examples of recent insider threat attacks, what failed, and techniques that work to address insider threat will be discussed.

Mr. Albert (Al) Lewis has 29 years of experience in systems integration, network security operations, and risk management. For the past 15 years, he has led information security teams for the DoD, Energy, and the Supreme Court. He currently serves as Principal Examiner for the Federal Housing Finance Agency (an independent regulatory agency) where he helps to ensure the safety and soundness of the Federal home loan mortgage and banking system. He has an MS Information Systems Management from Johns Hopkins University, and is a Certified Information Security Manager (CISM) and a Certified Information Systems Security Professional (CISSP).

Awareness: An Anti-virus Program for Humans

Gretchen Morris, CISSP, Technical Training Consultant, DB Consulting Group, Inc.

This session will cover best practices for an information security awareness program. It includes a variety of many interworking pieces that help support a holistic approach. This approach will help ensure that the recipients keep their guard up against the threats of today. Come to hear if there is something new you can implement or add to your awareness program as well as to share if you have something new in addition to what is presented.

Gretchen Morris is an IT Security Specialist for Federal Contractor, DB Consulting Group, Inc. For the past 15 years, she has supported the NASA IT Security Awareness and Training Center. With more than 20 years of teaching and troubleshooting experience on a variety of software packages and hardware configurations, Gretchen holds a Bachelor of Applied Science in Resource Management degree from Troy State University. Additionally, she earned the Master Training Specialist designation while serving as a Navy Instructor and has maintained CISSP certification since June 2002.

General deterrence theory, the individual, and what the cybersecurity person needs to know

Charles Wade, PhD Candidate, DSD Labs

It is known that by increasing cybersecurity knowledge, there is a decreasing likelihood an IT user will behave contrary to organizations norms. However, some individuals will have a paradoxical increase in undesired cybersecurity behavior. This is contradictory to GDT and can be caused by in increased risk tolerance in the IT user.

Charles Wade is a PhD candidate in Information Technology with a concentration in Cybersecurity. Currently, he is a Senior Security Engineer with DSD Labs, supporting the Headquarters Air Force Logistics, Engineering & Force Protection Division. Over the past six years he has assisted the Department of Defense and Air Force transition to the Risk Management Framework as a technical advisor and researcher from its inception. During his cybersecurity career he has served as an Information System Security Manager and as a Security Control Assessor Representative.

Visit the Vendor and Federal Agency Exhibition during the lunch break in the poster hallway
FISSEA Security Contest Entries in West Square

The Challenge of Creating an Adaptive Awareness Program

Tom Pendergast, Ph.D., Chief Strategist, Security, Privacy, and Compliance, MediaPro

One of the most provocative elements of the NIST Cybersecurity Framework for Awareness professionals is the challenge to develop a Tier 4: Adaptive program. For security professionals with constrained budgets and limited personnel—ring a bell, anyone?—building an Awareness Program that incorporates continuous improvement and "actively adapts" to changing threats can seem impossible. But it doesn't have to be that difficult! By leveraging free or inexpensive resources, you can deploy measurements that help you understand your risk posture, plan a sophisticated program, and deploy flexible (and often inexpensive) training and reinforcement communications to address your most pressing issues, creating a more risk-aware culture along the way.

This presentation will offer a conceptual model for how you can increase the flexibility and the visibility of your program, while focusing on some very practical things that you can do within a limited budget, all while driving toward a Tier 4 standard.

Tom Pendergast, Ph.D., has worked with hundreds of companies to develop and deploy Security, Privacy, and Compliance Awareness programs. He is the Chief Strategist for Security, Privacy, and Compliance at MediaPro, and the lead architect of the Adaptive Architecture™ approach to delivering data protection and compliance training and reinforcement. Tom has spent his entire career in content and curriculum design, first in print as the founder of Full Circle Editorial, then in eLearning with MediaPro. He received a Ph.D. in American Studies from Purdue University, and is the author or editor of 26 books and reference collections. Tom's hobbies include mountain climbing, photography, and reading.

Social Networks: Unsafe at Any Speed?

Carl Willis-Ford, Senior Principal – Solution Architect, CSRA, Inc.

Social Networks, from MySpace to Facebook to LinkedIn, are viewed as critical to modern life or the bane of privacy and security, or anywhere in between. The reality is that, like any privacy or security decision, the use of Social Networks should be based on risk management. This presentation takes a look at some of the most popular Social Networks, reviews the risks involved, and provides guidance for managing risks.

Carl D. Willis-Ford - Currently a Senior Principal – Solution Architect at CSRA, Inc. (created by the recent merger of SRA and CSC's Government Services). Formerly a nuclear reactor operator on fast attack submarines in the US Navy. Post-Navy, he taught nuclear reactor theory at Puget Sound Naval Shipyard until moving to IT as a database administrator. He started with SRA in 1997. Carl has 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 is currently in a Doctorate program in IA at the University of Fairfax. He mentors graduate students in both Technology Management and Management of Secure Information Systems programs at GMU and has taught graduate and undergraduate courses as adjunct faculty. He's presented on data security, software assurance, social engineering, and security governance topics to international, regional and state Oracle Users Groups, the Executive MBA program and Cybersecurity Innovation Forum at GMU, and the FISSEA conference. He serves in the Technical Working Group for FISSEA, and as a Program Committee Member for the IEEE International Big Data Conference. Awarded for Individual Excellence at SRA for 2013 and named a Senior Member of ISSA in January 2014.

The missing link in your security awareness program…. Internet Tradecraft!!

Russ Haynal, Expert Internet Instructor & Speaker, Information Navigators- Sole Proprietor

Slides may not be posted.

You have hammered your users about phishing, malware, USB devices, and Social Media… but what about Internet Tradecraft? Your employees are leaking all kinds of sensitive information through their everyday use of the Internet. These leaks can be as bad as a locally installed spyware program. Imagine a foreign adversary, or news reporter wandering around your workplace, looking at your employee's screens! This eye-opening session will discuss the OPSEC issues with http_referrer, which transmits a 1-click history to websites. Discover the evils of Google's cache /archive.org, web bugs, and email trackers. Do your employees even know what their Internet "persona footprint" looks like on a website? Internet tradecraft methods are presented that all users should know to protect your unclass networks (including mis-attributable persona).

Russ Haynal. Since 1994, Russ has provided customized Internet training to over 30,000 professionals from over 100 organizations, including all 17 agencies of the Intelligence community, all branches of the U.S. Military, numerous international partners and companies that support the IC. He has developed a series of courses focused exclusively on Internet Open Source research (OSINT), Internet OPSEC/tradecraft, and cyber security awareness. His course "Hidden Universes of Information on the Internet" is an elective for anyone trying to advance their career by completing the ICAAP (Intelligence Community Advanced Analyst Program). His initial clients also included Internet providers and telecom equipment manufacturers such as UUNET/MCI/Verizon, AT&T, Teleglobe, AOL, Bell Atlantic, Lucent Technologies and Newbridge Networks. Russ has presented at many events such as nine annual National OPSEC Conferences. He is also a founding officer of the Washington DC Chapter of the Internet Society.

Information Assurance for Executives & System Owners

Michael Petock, Cybersecurity Training Subject Matter Expert, US Department of State, Information Assurance Branch (OBXtek Inc.)

This presentation provides training for System Owners on information assurance and security best practices. It also covers the National Institute of Standards and Technology (NIST) guidance for role-based training that will assist System Owners in performing their jobs. The training features checklists and job aids, as well as scenario-based problem-solving exercises.

Particularly:

- System Owner tasks identified in the Risk Management Framework (RMF)
- The role of the System Owner within the Certification and Accreditation process
- How to assess the potential impact on an organization resulting from the loss of availability, integrity, or confidentiality of its information
- DOS and NIST Certification and Accreditation guidelines

Mike Petock. Since 2002, Mike Petock has supported the U.S. Department of State's Information Assurance (IA) training program as a trainer and Subject Matter Expert. He designs, writes, and teaches instructor-led, role-based Information Assurance courses for roles such as Systems Administrators, Information System Security Officers, IT managers, System Owners, and Executives. Through the U.S. Department of State's Information System Security Line-of-Business program, Mike has supported enterprise IA training programs with DHS, SSA, FBI, and NARA.

As the author of both of DOS's System Owner and Executive courses, Mike has an interesting insight into what should be included, how to present the information, and how to get the audience to attend the role-based training course. He will be sharing that insight during this session.

Last Chance Visit the Vendor and Federal Agency Exhibition during the afternoon break

Panel: The un-hackable human myth: Transforming goals of cyber education to reflect the reality of future threats

Dan Waddell, (ISC)^2, Moderator
Dr. Robert (Rocky) Young, Principal Cyber Security Engineer at MITRE
Christina L. Phibbs, Lead, Cyber Security Engineer at MITRE
Peter Gouldmann, Director, Office of IT Security Compliance, Directorate of Information Assurance, Bureau of Information Resource Management, U.S. Department of State

While a noble concept, if we center our education and training approach around the goal to attain "un-hackable" status, we will likely see a decline in the effectiveness of our students to combat future cyber threats. The manner and speed by which the world is adopting technology has outpaced our collective ability to implement adequate security measures. Everything from heart monitors and morphine drips to HVAC units and garage door openers are being hacked, with no end in sight to an expanding IP-enabled footprint. As cybersecurity educators, a shift must take place -- from training the cybersecurity workforce to training the workforce on cyber. We must set realistic expectations in the classroom and transform the goals of cyber education to reflect the reality of future threats.

This session will initiate a deep dive discussion among federal educators about how they are positioned to meet the educational needs of the future: the short- and long-term evolution of curriculum, redefining and expanding the education recipient profile, understanding the changing role of the information security professional, distinguishing those whose input is critical in the design of an effective program, and what all of this means to the maturation of an organization's overall workforce training concept.

Dan Waddell, CISSP, CAP, PMP, (ISC)^2 Managing Director, North America Region and Director of U.S. Government Affairs
Mr. Waddell is responsible for managing operations in the North America Region, which primarily focuses on supporting our U.S. and Canadian members, customers and strategic partners. He also leads all U.S. Government Affairs activities and is the primary (ISC)^2 official responsible for interacting with public sector entities (i.e. federal, state and local governments); major corporations; universities and other higher education institutions; and professionalization organizations throughout the U.S. Mr. Waddell serves as the principal point of contact for various trade associations; public interest groups and other entities focused on information security and information security workforce issues. He has over 20 years of experience in information technology, information assurance, and cybersecurity, with over 15 of those years in management.

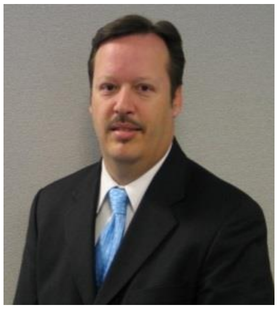
Mr. Waddell has been a featured guest speaker on cybersecurity issues on both TV and radio shows such as "NBC News4 Midday", "Government Matters" and "Federal News Radio", in addition to several cybersecurity conferences across the United States. He is currently a Fellow at the Institute of Critical Infrastructure Technology (ICIT), a non-partisan think-tank based in Washington, D.C. that acts as a conduit between the legislative community, technology providers and federal agencies. Mr. Waddell also chairs both the (ISC)^2 U.S Government Advisory Council and the U.S. Government Executive Writers Bureau, and received the (ISC)² President's Award in 2013.

Dr. Robert (Rocky) Young is an expert on cyber security, Information Assurance (IA) and Information Operations (IO). He has presented widely on issues and challenges related to the security of wireless/mobile devices, cloud/virtual networks, the cyber workforce, network/systems security principles, safeguards, and practices. Presently he is a Principal Cyber Security Engineer at the MITRE Corporation, a not-for-profit company that operates multiple federally funded research and development centers (FFRDCs). Dr. Young is supporting numerous U.S. Government sponsors with cyber security and cyber medicine initiatives, in addition to supporting numerous corporate endeavors. Previously as a government civilian, he supported the Secretary of Defense as the Director for Cybersecurity and Information Assurance Outreach (CIAO) and Mobile Device Security Division, Office of the DoD Chief Information Officer. Dr. Young has been a professor at National Defense University since 2002. Prior to that, he was Chief of 11th Wing Information Assurance Office, Air Force District of Washington, providing policy guidance, technical support, and security oversight of communication, computers, and classified emissions. Dr. Young retired from the USAF after serving on active duty for 21 years, starting with his enlistment at seventeen from the Upper Peninsula of Michigan. In the beginning of his career he served in the Middle East/Desert Storm, mid-career he was selected to serve as Aircrew for the White House, and ultimately finished up his military career as a Commissioned Federal Medical Officer. He continues to serve as a volunteer in his Medical Officer capacity with the Wounded Warrior Program at the Walter Reed National Military Medical Center and teaches masters-level cyber security courses at the University of Maryland and Syracuse University

Christina Phibbs is a Lead Cyber Security Engineer, for Strategy, Policy, and Privacy within the Cyber Security Technical Center at the MITRE Corporation. MITRE is a not-for-profit organization operating federally funded research and development centers (FFRDCs) for the government. Her work focuses on cyber security measures of effectiveness (MOEs) and scorecards, security in healthcare, and cyber security workforce. Christina has more than 20 years of professional experiencer supporting various Defense agencies in the areas of computer network defense, threat intelligence analysis, network vulnerability assessments, compliance inspections, enterprise-wide cyber incident response and reporting, and strategic planning. She was a key member of the team that established the Information Assurance

Technology Analysis Center (IATAC), serving as the promotional director for more than 10 years. In this capacity, she was editor-in-chief of the *IAnewsletter*, coordinated the development and production of numerous technical reports, and established and maintained the institution's community engagement program.

Christina earned an M.S. with distinction in Information Systems and Technology Management, concentrating on Information Assurance and Security (IAS) from Capella University in 2015, and is currently a doctoral candidate in Information Technology with the same concentration.



Peter Gouldmann is Director of IT Security Compliance for the U. S. Department of State. In this role he oversees risk identification and management to Department of State operations arising from its use of information technology. Pete directs teams responsible for security control assessments, compliance reporting and Office of Inspector General and Government Accountability Office IT security engagements.

Pete's 30+ years of IT and security experience spans public, private, domestic and global organizations as well as the United States Air Force. He holds a Masters Degree in Information Management, a Bachelor of Science in Management, and is a distinguished graduate of the National Defense University's Advanced Management Program. Pete has been awarded the CIO certificate in Federal Executive Competencies from the CIO University, and holds the Certified Information Systems Security Professional (CISSP) credential and Project Management Professional (PMP) certification.

Pete is an expert, and often speaks on and has authored articles on the topic of information risk management. He was a past co-chair of the Committee on National Security Systems permanent subcommittee and a member of the NIST Joint Taskforce Transformation Initiative Interagency Working Group. Pete co-chairs the (ISC)^2 Government Advisory Council and is an assistant adjunct professor for the University of Maryland University College.

Awareness to Action: Advancing Human Defense

Ellen Powers, Cybersecurity Threat Awareness Lead, The MITRE Corporation

Slides will not be posted.

Everyone clicks, even those who recognize the signs of suspicious email. So, how can you shore up your defenses while bolstering your detection capabilities, especially amid advancing cyber adversary tactics and targeting? And how can you grow your human sensor network to include employees not previously engaged in spotting or reporting email? This talk will touch on the work culture needed to germinate the employee-as-human-sensor, the metrics that illustrate its effectiveness, and a voluntary pilot program aimed at converting non-reporters into reporters, clickers into self-reported clicks, and targets into human sensors, thus extending the human sensor network and employee as cyber defender.

Ellen Powers started a human sensor network for The MITRE Corporation back in 2009. As a cyber security threat awareness leader, her work analyzing cyber threat attacks has led to a network of employees that can detect advanced cyber attacks before network-based sensors and signatures. She continues to work in the intersection of cyber threat analysis and human defense to address the range of prevention, detection, and cyber intelligence needs of the company and community.

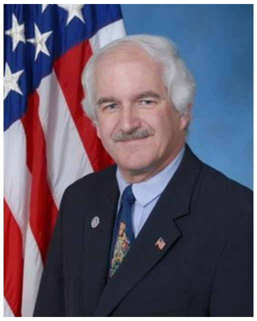
Cyber Ethics

Craig Holcomb, NSA Compliance Officer (Retired), National Security Agency

Slides will not be posted.

Cyber ethics refers to a code of safe and responsible behavior for the Internet community. Practicing good cyber ethics involves understanding the risks of harmful and illegal behavior on-line. The information presented will help students understand the ethical issues as related to computers. Terms will be introduced and cases will be presented to help the students understand the material. Topics that will be presented include: (1) Computers and Privacy; (2) Crime, Abuse, and Hacker Ethics; (3) Responsibility; and (4) Social Implications and Consequences. The students will leave with simple guidelines on how to make an ethical decision and the Ten Commandments of Computer Ethics.

Craig Holcomb retired as 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 was at NSA for over 34 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. Finally, he was NSA's Senior Compliance Officer, ensuring NSA complies with laws such as the Federal Information Security Management Act.

Mr. Holcomb was a speaker for NSA's Mathematics Speaker's Bureau for over 20 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 was a technical recruiter for over 19 years presenting information on NSA to high school and college students. He represented the skill field of Computer Science and was the Chair of NSA's Stokes Educational Scholarship Program Mentor Committee.

Unbundling Cyber Security: Integrating Cyber Security Awareness in K-12, Higher Education, and the Community

Dr. Edna Reid, James Madison University

Slides will not be posted.

With the increase in sophistication, frequency, and impact of cyber security incidents, there is a need to unbundle cyber security so that the focus goes beyond technology. It includes a paradigm shift in viewing cyber security as an organic system with interconnected components focusing on its interdisciplinary aspects.

This requires pushing cyber security awareness and training down the pipeline from the workplace, to higher education, K-12 students, teachers, and communities. It involves integrating it into the curriculum beyond technology and STEM courses to others such as civics, political science, and cultural studies. Plus, integrating it into the general community such as collaborating to organize Cyber Security Kiosk at local shopping malls.

With such a holistic approach, employees will be exposed to cyber security awareness from multiple perspectives such as parents learning from their children, as college students, and as community members. Furthermore, new employees, such as recent graduates, will come to the workplace with a heighten level of awareness to meet the needs for emerging specialists such as cyber threat analysts and cyber crisis communication specialists.

JMU is unbundling and integrating cyber security into other disciplines besides computer science such as intelligence analysis and crisis communications. For example, JMU used the Analyze category of the National Cybersecurity Workforce Framework to create new elective courses: (a) Cyber Intelligence and (b) Cyber Security Operations and Policies. Collaborating with industry, academic, and government, JMU is training K-12 educators and their students, business leaders, and government officials on integrating cyber security awareness into their areas.

Dr. Edna Reid is an associate professor in the Intelligence Analysis Program at James Madison University. In 2013, she retired as an intelligence analyst at the FBI. In 2013, she received a certificate in Denial and Deception (D&D) from the National Intelligence University (NIU). She is a member of the Cyber Intelligence Task Force at the Intelligence and National Security Alliance (INSA) and the Federal Information Systems Security Educators Association (FISSEA). Her areas of specialization are cyber intelligence, gamification, and cyber deception.

She taught at several universities in the U.S. and Singapore. At the University of Arizona, she served as a research scientist in the Artificial Intelligence Lab and domain expert on the Dark Web project. She was an Associate Professor with Nanyang Business School, Nanyang Technological University (NTU), Singapore. Formerly, she was an entrepreneur with an information brokerage company in Malaysia. Prior to coming to Asia, she was at Rutgers University. She was a postdoctoral researcher at the University of California, Berkeley, where she conducted research in terrorism information services. Before her Silicon Valley experience, she was a senior systems analyst and data analyst team leader at private enterprises in Germany and Northern Virginia. She has a doctoral from the

University of Southern California, MLS from the University of Maryland, Graduate certificates in (a) Management information System (MIS) from American University and (b) D&D from NIU, and a BS in Education.

4:55 Conference Close - Green Auditorium – Prize Drawings

FISSEA holds an annual conference every March. Plan ahead for 2017.

The Federal Information Systems Security Educators' Association (FISSEA), founded in 1987, is a volunteer organization run by and for federal information systems security professionals to assist federal agencies in meeting their information systems security awareness, training, education, and certification responsibilities. Vendors and contractors who work with and support federal IT security programs are also members, as are members of the academic community, state and foreign governments.

Patricia Toth is Chairperson of the Working Group. The Working Group members are from various agencies and organizations and volunteer their time.

Peggy Himes has worked with FISSEA Executive Boards and Working Groups since 1998.

FISSEA Working Group

Scott Anderson, Veterans Affairs (VA)
Dan Benjamin, American Public University
Terry Brox
Art Chantker, Potomac Forum
Brenda Ellis, NASA
Susan Farrand, Dept of Energy
Raymond Greenlaw, USNA
Angela Guinn, VA
Susan Hansche, DHS
Peggy Himes, NIST
Lewis Craig Holcomb, NSA, retired
John Ippolito, Consultant

Lance Kelson, Dept of the Interior
Albert Lewis, Federal Housing Finance Agency
Gretchen Morris, DB Consulting/NASA
Louis Numkin, FISSEA Life Member (retired IRS)
Loyce Pailen, UMUC
Edna Reid, JMU
Mike Riley, EdgeSource/State
Kimberly Sanders, Amtrack
Cheryl Seaman, National Institutes of Health
Pat Toth, NIST, Chairperson
Jim Wiggins, Federal IT Security Institute
Carl Willis-Ford, CSRA
Mark Wilson, FISSEA Life Member (retired NIST)

Thank you.....

- **Speakers for donating their time, energy, and knowledge.**
- **Attendees. We hope you found our conference of value.**
- FISSEA Working Group members for their input on the program and assisting with on-site details.
- Gretchen Morris for coordinating the FISSEA Security Contest.
- NIST Applied Cybersecurity Division and/or Computer Security Division support:
  - Patricia Toth, Conference Chairperson
  - Peggy Himes, Conference Administrator
  - Kevin Stine, Division Chief for Applied Cybersecurity Division
  - Nicole Keller, website updates and designing the program cover
- NIST Public Affairs Office: Mary Lou Norris, Karen Startsman, Crissy Robinson, Jami Schwartz, NIST AV Technicians including Joe Hynes.
- The Federal Business Council: Lindsay Smith and George Hall.
- American Public University for donating bags and water bottles for all attendees – Dan Benjamin.
- Prize drawing contributors:
  - SANS - two Amazon Fire tablets
  - Art Chantker - Certificates for Complementary Attendance at Any Potomac Forum Training Workshop (or two day workshops) Value up to $1400. Some Workshops are Government Only
  - Carl Willis-Ford - Kindle Paperwhite, 6" with Built-in Light, Wi-Fi
  - Peter Coddington, CMDSP - Credentialed Mobile Device Security Professional - gift certificates for the Vendor Bingo game winners
  - Al Lewis (hardcover book): “The CERT© Guide to Insider Threats” (Capelli, Moore, Trzeciak, Carnegie Mellon Software Engineering Institute), Addison-Wesley, 2012.
  - Pat Toth – NIST apparel
- Conference presentations, receiving permission, will be posted after the conference.
- FISSEA Website: http://csrc.nist.gov/fissea
- To be added or removed to the mailing list (fisseaupdates@nist.gov), email fisseamembership@nist.gov – conference attendees will be automatically subscribed.

NOTES

NOTES

fissea

Federal Information Systems Security Educators' Association

AWARENESS • TRAINING • EDUCATION

www.csrc.nist.gov/fissea
National Institute of Standards and Technology