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

28th Annual Conference

"Changes, Challenges, and Collaborations: Effective Cybersecurity Training"
National Institute of Standards and Technology
Gaithersburg, Maryland

2015 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 24, 2015

Conference Welcome – Patricia Toth, NIST, Conference Chair

Pat Toth is a Supervisory Computer Scientist in the Computer Security Division at NIST. Her current project areas include information security, cybersecurity awareness, training and education. Pat is the lead for the FISMA team, Chair of the FISSEA Technical Working Group, 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 – Charles H. Romine, Ph.D., Director, Information Technology Lab

Charles Romine is Director of the Information Technology Laboratory (ITL). ITL is one of six research Laboratories within the National Institute of Standards and Technology (NIST) with an annual budget of $120 million, more than 350 employees, and about 160 guest researchers from industry, universities, and foreign laboratories.

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: Information Security System Educators Must be Leaders

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

This talk will address issues consistent with the conference theme of changes, challenges, and collaborations for effective cybersecurity training. The key changes to be highlighted are that: everything is now on line; everything on line can be hacked; and cybersecurity is more important than ever. The key challenges for cybersecurity educators are to: capture users' attention; motivate users to follow cybersecurity practices; and earn users' respect. The key collaborations must now be with everybody on an "individual" basis. To achieve these goals, information security system educators must become and be perceived as meaningful leaders. How to achieve this status and role will be discussed.

Neil E. Grunberg, Ph.D., is Professor of Military & Emergency Medicine, Medical & Clinical Psychology, and Neuroscience at the Uniformed Services University of the Health Sciences (USU) in Bethesda, Maryland, where he helps to train physicians, psychologists, nurses, scientists, and educators to serve in the armed forces, the Public Health Service, or in academic positions. He also is Director of Leadership Programs in the USU School of Medicine. Dr. Grunberg earned baccalaureate degrees in Medical Microbiology and Psychology from Stanford University (1975). He earned M.A. (1977), M.Phil. (1979), and Ph.D. (1980) degrees in Physiological Psychology and Social Psychology from Columbia University and completed Ph.D. training in Pharmacology at Columbia University's College of Physicians & Surgeons. He has published more than 160 scientific papers on stress, substance use and abuse, behaviors related to physical and mental health, and leadership. Dr. Grunberg has received scientific awards from the U.S. Surgeon General, Centers for Disease Control, U.S. Food & Drug Administration, American Psychological Association, and Society of Behavioral Medicine. He has received more than a dozen awards for medical school and graduate education and contributions to the Uniformed Services University. Dr. Grunberg is honored to be selected as a 2015 Presidential Leadership Scholar. Dr. Grunberg spoke at the 2009, 2010, and 2012 FISSEA meetings. His keynote address to the 2015 FISSEA meeting is entitled, "Information Security System Educators Must Be Leaders."

Security Awareness Smartcuts

K Rudolph, Founder and Chief Inspiration Officer, Native Intelligence, Inc.

This story-based presentation provides strategies to help FISSEA members use "smartcuts" to design better training. Audience members will receive tips and techniques for creating tightly-focused, results-oriented eLearning for adults. This presentation will address the difference between smartcuts and shortcuts. We'll also discuss three smartcuts for creating training that is sticky (memorable) and effective (prevents loss). Audience participation is encouraged as this presentation will include fabulous prizes. A handout will be available on the FISSEA site after the conference.

K Rudolph is the founder and Chief Inspiration Officer at Native Intelligence, Inc., a firm that provides award-winning, effective, and entertaining security awareness courses, programs, and materials. K believes that security concerns are best addressed by well-prepared and security-savvy individuals. She enjoys being involved in security training, education, motivation, and awareness activities.

K is especially interested in the psychology of security awareness and influence as related to learning and behavior, storytelling, and security awareness metrics.

K is a Certified Information Systems Security Professional (CISSP) and Federal IT Security Professional (FITSI-M) with a degree from Johns Hopkins University.

K's publications include: System Forensics (co-authored with John R. Vacca) and Jumpstart to Computer Forensics (coauthored with Michael Solomon, Ed Tittel, Neil Broom, and Diane Barrett). K is the primary author of the chapter on security awareness from the Computer Security Handbook, Vols. 4 and 5 and 6 (2014). She is also the author of the chapter on security awareness in the three-volume Handbook of Information Security published in 2009 and 2006. K was the Technical Editor for Fundamentals of Communications and Networking (2014) and Security Strategies in Windows Platforms and Applications. In 2015, K served as a Subject Matter Expert for Jones & Bartlett's Mobile Device Security text.

In March 2006, FISSEA honored K as their Security Educator of the Year. K is also a named contributor to and participant in the work group that created NIST Special Publication 800-16, **Information Technology Security Training Requirements: A Role-and Performance-Based Model.**

K is a volunteer with (ISC)²'s **Safe and Secure Online** program, which brings awareness presentations for 11-14 year-olds and for parents and teachers to local schools.

Why Gamification is Winning Strategy for Information Systems Security Training

John Findlay, Founder, Launchfire

By the end of this session you'll have a solid understanding of gamification and why it works so well for training. Plus, you'll have some great ideas that you can implement on your training programs.

Let's face it; most people aren't itching to take information systems security training. So, what's the most effective way to get people to do something they don't want to do? Turn it into a game!

In this fast-paced session you'll learn how to gamify your training programs to make them more magnetic, more engaging, more fun and more effective. You'll learn what game tactics have been successful at prompting initial participation and which ones have been effective for driving comprehension and retention.

Don't miss this session. You need to get in the game!

John Findlay is a founding partner of the gamification shop, Launchfire. Early in life John showed promise in the non-existent field of gamification making games out of everything from homework to chopping wood.

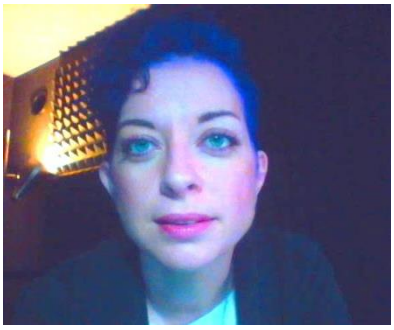
Stuck with the unenviable task of training all-knowing upper management to use SAP John discovered a professional use for his otherwise useless proclivity. He found that by making games out of the content he was able to get folks more engaged. It was then that he knew he was on to something.

John went on the start Launchfire where he's created gamified training programs for the likes of Dell, Intel, Microsoft, Jet Blue, Marriott and tons more.

Changing Behavior through Risk Management

Sandra Marie Toner, Technical Specialist, ICF International

This presentation delineates risk management practices currently in use and shows how they have transformed existing prescribed processes. Ms. Toner will explain how focusing on risk can result in more adaptable processes that result in better visibility over agency environments. She will highlight how aligning security awareness with a risk-based approach can solve a persistent problem- end-users choosing convenience over security. Finally Ms. Toner will offer some suggestions on how to pinpoint behavioral changes in end-users by incorporating targeted risk management education in a cybersecurity training program.



Sandra Toner is a Technical Specialist at ICF International. She works on Governance, Risk, and Compliance programs across various industries. Ms. Toner has a M.A. in Leadership in Teaching with a concentration in Technology and she is a CompTIA Certified Technical Trainer (CTT+).

Up Your Game: Utilizing the Understanding by Design Framework to Maximize the Effectiveness of Cybersecurity Training Programs

Kristi A. Aho, Senior Security Trainer, Wyle Science, Technology & Engineering

From data breaches at major retailers to cyber warfare attacks, malware infections, or even social media privacy settings, mainstream media news about cybersecurity is increasing in both profusion and intensity. For cybersecurity educators, cutting through the noise is a major challenge. It is no longer enough to simply provide the information our target audiences need to know. In order to be effective, we must present the information in a concise format that captures attention in a relevant and meaningful way.

Understanding by Design (UbD) is a popular educational planning tool developed by Jay McTighe and Grant Wiggins. Its "backward" design process has been widely adapted for use in a variety of educational settings. UbD starts with identification of enduring understandings and desired outcomes and results in learning that will transfer to new situations and have lasting value beyond the boardroom or classroom.

Whether the goal is briefing leadership on an organization's cyber risk exposure, providing cybersecurity professionals with new skills to counter emerging threats, or delivering mandated awareness training to end-users, attendees will learn how the UbD framework can be a valuable guide in the design and presentation of training materials that are highly effective, focused and compelling.

Kristi A. Aho is passionate about promoting Cyber Security Training and Awareness among IT users at all levels. She has over 20 years of experience in IT Systems and Security Engineering, training, and education. As a Senior Security Trainer with Wyle Science, Technology & Engineering, Ms. Aho is currently developing a comprehensive training package covering the security infrastructure and tools utilized by the ground segment of the NOAA/NASA GOES-R weather satellite. Prior to joining the GOES-R project at Wyle, Ms. Aho worked for over 13 years at the Johns Hopkins University and Medical Institutions, holding a series of increasingly responsible positions in departmental and enterprise-wide IT Systems, Cyber Security, and IT Project Management. She has developed and taught Cyber Security, Networking, and Industry Certification courses both full-time and as a part-time adjunct professor at Howard Community College in Columbia, Maryland.

Ms. Aho has a Bachelor of Science degree in Mathematics from the University of Maryland at College Park and a Master's Degree Adult Learning and Online Teaching and Learning from the Johns Hopkins University. She holds multiple professional certifications including Certified Information Systems Security Professional (CISSP) and Project Management Professional (PMP).

Spear Phishing: Exercise to Reduce Your Risk

Deborah Coleman, Department of Education

Note: Slides will not be posted.

Over the past year, many of the data breaches in news media headlines began with something as simple as an email message. Carefully crafted spear phishing email messages tricked unsuspecting end users into taking action. Users provided their user name and password, clicked a link to a malicious website, or opened a malware laden email attachment. These actions enabled the attackers to remotely control the user's computer and gain undetected access to organizational systems and information – often for long periods of time.

Spear phishing attacks continue to grow in both frequency and sophistication. In fact, the United States Computer Emergency Readiness Team (US-CERT) and National Security Agency (NSA) both identified phishing as one of the top threat vectors putting Federal Departments and Agencies at risk. To counter this serious threat, it is important for users to understand, be able to identify, and be able to protect themselves from phishing attacks. This presentation provides information on developing and implementing a simulated phishing exercise program and the benefits gained by the U.S. Department of Education by building emerging threat exercises into their awareness and training program.

Deborah Coleman is a 25+ year information technology management veteran of the U.S. Department of Education. Since 2004, she has been actively involved the development and oversight of the Department's Cyber Security Awareness and Training Program. This robust program provides awareness and training to over 10,000 federal employees and contractor personnel with access to the Department's sensitive systems and information. She oversees the development of the Department's mandatory Cyber Security and Privacy Awareness courses, Department specific specialized role-based training courses, and communications materials that promote awareness including posters, newsletters, brochures, and job aids. Under her direction, the Department's program has expanded to include a role-based Professional Development Program for personnel with cybersecurity responsibilities and spear phishing exercises. She is a certified Project Management Professional (PMP) and holds a B.S. in Criminal Justice and a Masters of Public Administration from the Pennsylvania State University.

Prize Drawing	**Presentation of FISSEA Security Contest Winners** **by Gretchen Morris, Contest Coordinator**
1:05 – 1:40 pm Green Auditorium	**2014 FISSEA Educator of the Year Presentation** **Presented by Sam Maroon, 2013 FISSEA Educator of the Year**

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) 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 coordinated this contest and enlisted an impartial judging committee.

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

FISSEA Educator of the Year Award

FISSEA recognizes an individual who has made significant contributions in education and training programs for information systems security. Nominees may be involved in any aspect of information systems security awareness, education, or training, including, but not limited to, instructors, security program managers, and practitioners who further education and training programs for information systems security in the public, private, or federal community. Nomination information and a list of previous recipients are available on the website, http://csrc.nist.gov/organizations/fissea/educator-year/recipients.shtml

We were honored to award **Sam Maroon**, the 2013 FISSEA Educator of the Year at the March 2014 Conference. Mr. Maroon received this award for his tireless work in training our Nation's injured servicemen and woman in transitioning them to the cyber battlefield through an academy known as the Wounded Warrior Cyber Combat Academy (W2CCA). He has donated no fewer than 300 hours of his own personal time to train members of Cyber Team 1.

Using IoE to Give Awareness Training a Fresh Start

Dan Waddell, CISSP, CAP, PMP, Director of Government Affairs, (ISC)2

The impact of the Internet of Everything (IoE) on government is still greatly unknown, but similar to the mobile technology initiative, government finds itself having no choice but to participate. As the promise of the IoE emerges across government, security awareness training must rise to a whole new level. With computer-driven cars, HVAC systems, heart monitors, appliances, etc. joining the ranks of networked devices, threats to our physical safety quickly multiply. As a result, organizational leaders are asking how do we make users aware of the potential dangers that exist in the daily operation of these systems? How do we address security awareness with the proliferation of "everything" coming online?

The good news is that IoE represents an opportunity for organizations to give their security awareness training program a fresh start. Security awareness training is considered a key component of an organization's overall security program. Given the potentially enormous impact of the IoE, relevancy and retention is key. So where do organizations start?

Organizations must recognize that education and training needs require a broader strategy than most envision. People throughout their organizations -- from the end user to everyone that works with IT that provides access to or hosts information assets -- plays a key role in information security.

We need to build our security awareness program around an ongoing series of interactive communications geared towards this broad user base, rather than sending out a PPT file once a year. Ultimately, IoE security awareness training should paint a picture; starting with a full outline of what's to come, adding color to areas of progress, and illuminating a background that gives dimension to its potential dangers.

Mr. Waddell has over 20 years of experience in information technology, information assurance, and cybersecurity, with over 15 of those years in management. He is an experienced cybersecurity program manager and subject-matter expert for multiple disciplines and skill areas including CISO/CSO advisory services, secure cloud computing, privacy, data loss prevention, regulatory compliance, threat and vulnerability assessments, incident response, disaster recovery/business continuity and risk management. He is currently the co-chair of both the (ISC)² North American Advisory Board and the Government Advisory Board for Cyber Security, providing guidance and expertise on pressing information security policies and trends and recommendations regarding (ISC)² professional certification and education programs. Mr. Waddell is also a frequent speaker, contributor and volunteer on several cybersecurity-related initiatives including our Safe and Secure Online program, and is a 2013 (ISC)² President's Award recipient.

Six Approaches to Creating an Enterprise Cyber Intelligence Program

Joshua Ray, CISSP, CEH, Senior Director, Verisign iDefense, Verisign

Cyber intelligence has matured from an industry buzzword to a formal discipline, which has implications for vendors and security leaders. As few as seven years ago, cyber-threat intelligence was the purview of a small handful of practitioners, limited mostly to only the best-resourced organizations and defense and intelligence agencies involved in computer network operations. Fast forward to today, and just about every business, large and small, is dependent on the Internet in some way for day-to-day operations, making cyber intelligence a critical component of a successful business plan. This presentation explores the wide variety of ways organizations can go about creating a cyber intelligence program.

Joshua A. Ray As Senior Director for Verisign iDefense, Josh is responsible for the company's enterprise Cyber Intelligence Program as well as the operations and product strategy for the iDefense business. He has 14 years of combined commercial, government and military experience in the field of cyber intelligence, threat operations and information security. Prior to his work with Verisign, Josh created and managed the Cyber Threat Operations Intelligence Program at Raytheon, which handled enterprise-wide intelligence activities focusing on defining and providing early warning of advanced cyber threats targeting Raytheon's networks. Josh also held technical leadership roles with the Office

of Naval Intelligence (ONI) and the Northrop Grumman Corporation at the Joint Task Force – Global Network Operations (JTF-GNO), providing intelligence support to focused operations. Josh is a recognized cyber intelligence expert within the US Department of Defense (DoD) and intelligence community on matters relating to cyber exploitation and adversarial tactics, *techniques, procedures and technologies and for his work on computer network exploitation* and cyber adversarial actions. Josh has been credited for his work on intelligence community assessments related to cyber threats and has presented at a variety of DoD and commercial cyber intelligence conferences and symposiums. Josh holds a Bachelor of Science in information technology from George Mason University, an Executive Certificate in strategy and innovation from MIT Sloan School of Management and served honorably as a member of the US Navy.

21st Century Classroom Techniques

Sergeant Major Kevin E. McCrary (retired) Army Office of the Chief Information Officer/G-6; Christopher Bloor, Vice President of Global Cyber Programs, Logical Operations

With the evolving threat of cybercrime looming over the government and corporate world alike, innovative approaches to security training are needed to ensure the safety of our networks. No longer is a degree, a certification, or relevant work experience enough to prepare for the array of threats we face. Information assurance professionals require constant access to relevant, job related training in preparation for the growing wave of attack vectors targeting our networks. The key is in developing an understanding of cybersecurity as an ongoing discussion or topic; not solely the products and courses we currently rely on today. To match the threats we face, we must move beyond learning in the traditional classroom, allowing those in the field to apply their training in the real world, in real time.

Sgt. Maj. Kevin E. McCrary became the Army Chief Information Officer/G-6 Senior Enlisted Adviser on February 22, 2011. Sgt. Maj McCrary serves as the Army's CIO/G-6's personal adviser on all enlisted matters in areas related to Information Technology affecting operations and Soldier training and quality of life across the Army.

He has held a variety of leadership positions throughout his career from Signal Team Chief, Section Sergeant, Shift Supervisor, Platoon Sergeant, First Sergeant, Drill Sergeant, Senior Drill Sergeant, Equal Opportunity Advisor, Training and Operations Officer to a nominative position as Operations Sergeant Major, White House Communications Agency.

Christopher Bloor has extensive experience in the public and private sector in the learning and technology field. With over 20 years of experience, Mr. Bloor is a leader in learning and training & development with an emphasis in technology education. Additionally, Mr. Bloor is a recognized thought leader and public speaker in the learning field and has spoken at RSA and EC Council's Hacker Halted.

As Vice President of Logical Operations, Mr. Bloor provides strategy and business development services to public and corporate clients. He works with clients to determine best practices to achieve their goals and find efficiencies in implementing their long-term strategy. This is accomplished by improving performance and operations, supporting internal talent and building strategic alliances.

Educating the End User on Mobile Device Security

Dr. Karen Paullet, American Public University

The increased use of mobile devices has led to an increase in security threats. Only a small percentage, approximately 4%, of mobile devices is protected by security and anti-malware software. Protecting personal and company information has become an area of concern as increasing numbers of people use mobile devices. Security risks are on the rise as a result of end user behavior, as organizations continue to become more dependent on mobile devices. What security mechanisms do we have in place to deal with mobile security threats? Are Bring Your Own Device Polices (BYOD) needed with an organization? In order to protect personal information, users must become aware of the risks associated with using mobile devices.

Dr. Paullet's goal is to educate end users and provide tips to implement within their organizations.

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 D.Sc. 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.

Why Your Security Education Program Isn't Working

Ralph Massaro, VP of Sales, Wombat Security Technologies

If you've been running annual security awareness events using the best video you could find and you're not seeing a change in behavior it's time to stop and re-evaluate what you're doing. It's not that security awareness and training doesn't work, it's that you need to spend more time using the fundamental tactics that help people learn and apply those to your program.

If your training program has any one of these elements you need to attend this session to learn how to get your security education program measurably delivering results.

If your training program . . .

1. Only happens once per year
2. Is a slide presentation or a video that depends upon the end user sitting and listening
3. Tells the end user what to do but doesn't explain why
4. Is a session with a duration longer than 15 minutes
5. Focuses only on awareness but not behavior change

Then you need to attend this session to gain actionable advice about a Continuous Training Methodology that has been proven to reduce malware infections and phishing attacks from the wild up to 90%.

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

Proactive User Risk Management

Trevor Hawthorn, CTO & Co-Founder, ThreatSim

Leveraging dynamic training and simulations to achieve actual end user behavior modification. We will explore several case studies across our customer base to demonstrate how they utilize simulations and scenario-based training activities to re-wire end users' brains to become more security-minded. Lots of metrics along with do's and don'ts on how to include these activities in your security awareness program.

Trevor Hawthorn is the co-founder and CTO of ThreatSim, leading its DevOps and development teams. With over eighteen years of information security experience in both consultative and operational roles, Trevor brings a unique set of skills to ThreatSim. Prior to founding ThreatSim, Trevor was a Senior Security Consultant with Cybertrust (now Verizon Enterprise) where he performed technical information security assessments for organizations across multiple industries. Prior to Cybertrust, Trevor was part of UUNET's DDoS Attack Mitigation and critical infrastructure protection team. While at UUNET, Mr. Hawthorn delivered training to the FBI Training Academy at Quantico and other law enforcement groups. Trevor has presented at several industry security conferences on mobile and other advanced attacks.

Using NIST Cyber Security Framework to Encourage Board Discussions and ERM Oversight Function

Paul A. Ferrillo, Esq., Weil Gotshal & Manges LLP

Recently disclosed cyber attacks have indicated not only is data and IP theft a problem, but the destructiveness of the attacks to infrastructure (servers, telephones) can serve to bring down the affairs of major corporations. Many board members are still scared of cyber and are not plugged into to the hazards of failing to take heed of the current threat environment. They need to embrace the NIST cyber security framework as a method to continue cyber discussions and better improve their company's cyber defensive posture. The NIST framework can help. Here's how to roll out the framework to your board of directors in a fast efficient way to get the ball rolling to protect the enterprise from cyber attacks, and follow on litigation and regulatory actions. The reputational damage, business costs and loss of confidence of customers and investors are far greater perils than the time spent implementing the framework.

Paul Ferrillo is counsel in Weil's Litigation Department, where he focuses on complex securities and business litigation, and internal investigations. He is part of Weil's Cyber Security, Privacy, and Information Management practice, where he focuses primarily on cybersecurity corporate governance issues, and assists clients with governance, disclosure, and regulatory matters relating to their cybersecurity postures and the regulatory requirements which govern them.

Mr. Ferrillo has extensive experience in the area of directors' and officers' liability insurance issues by virtue of his prior employment with American International Group (AIG), in its major U.S. underwriting subsidiary, National Union Fire Insurance Company of Pittsburgh, Pa. (the largest writer of D&O insurance in the U.S.), where he held numerous senior-level positions in its claims and underwriting areas. He frequently counsels public companies and their boards of directors, private equity companies and their portfolio companies, and hedge funds on a vast array of issues relating to the nature, extent, types and availability of all D&O and Management Liability Insurance-related products, as well as on indemnification and advancement issues.

Mr. Ferrillo also regularly counsels clients in the growing field of cybersecurity corporate governance, which is an increasingly important part of a Board's enterprise risk management function. Mr. Ferrillo counsels clients on cyber governance best practices (using as a base the National Institute of Standards cyber security framework, which was announced on February 14, 2014), third-party vendor due diligence issues, cybersecurity regulatory compliance issues for Private Equity, Hedge Funds, and Financial Institutions that have been promulgated by the SEC, FINRA, the FTC, and the FDIC/OCC, the preparation and practicing of cyber security incident response plans, as well as evaluating and procuring cyber liability insurance to protect against losses suffered by companies as a result the theft of consumer or personally identifiable information, or as a result of the destruction of servers and corporate infrastructure.

The National Cybersecurity Workforce Framework: The Foundation for Building the Nation's Cybersecurity Workforce

Benjamin Scribner, Director, Cybersecurity Professionalization and Workforce Development Program, Department of Homeland Security (DHS), Cybersecurity Education & Awareness Branch (CE&A)

National Cybersecurity Workforce Framework (Workforce Framework) – The Workforce Framework defines cybersecurity work, Specialty Areas, knowledge, skills, and abilities (KSAs), and categorizes job functions. It can be used by numerous cross-sector organizations (e.g., private industry, educational institutions, etc.). The Workforce Framework has been updated to reflect the evolving cybersecurity field and changes in technology and incorporate diverse viewpoints and resonate across government, industry, and academia.
Link: http://niccs.us-cert.gov/training/tc/framework

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

Education and Awareness: Manage the Insider Threat

Carl Willis-Ford, Senior Technical Advisor, SRA International, Inc.

CERT categorizes Insider Threats as malicious (including intellectual property theft, IT sabotage, fraud, and espionage) or accidental. Research suggests that a nonmalicious category should be added alongside the other two categories. This presentation provides a look at some of the research covering how improving employee cybersecurity education and awareness can help manage the spectrum of insider threats.

Carl D. Willis-Ford Currently, a Senior Technical Advisor II at SRA International, Inc., doing capture and solution architect work. Formerly a nuclear reactor operator on fast attack submarines in the US Navy. Post-Navy, 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). He mentors graduate students in both Technology Management and Management of Secure Information Systems programs at GMU, and teaches undergraduate and graduate classes as adjunct faculty. He's presented on data security, software assurance, social engineering, and security governance topics to International Oracle Users Group conferences, the regional and state Oracle Users Groups, the Cybersecurity Innovation Forum at GMU, the IA club at Penn State, various commercial firms, and the FISSEA conference. Awarded for Individual Excellence at SRA for 2013 and named a Senior Member of ISSA in January 2014.

Bridging Technical and Business Domains for Effective Security Programs

Dr. Stephen C. Fortier, Northcross Group

The session will look at challenges of training and managing technical and business focused people working together in security programs. Each perspective has vital roles in reducing risk across the different security domains, but a lack of alignment can have the opposite effect. The session will leverage current research and examples of how technology and business work together—successfully and not--from a variety of industries. The session will present a model for security programs and training focused on integrating efforts and delivering measurable security value.

The session will present research of the Northcross Group and the George Washington University Institute for Crisis, Disaster and Risk Management that looks at the differences in how technical and business people work; and specifically in dealing with incidents versus regular projects and activities.

The session will look at program and training structures for communicating, working, and judging the value of efforts. Examples of program success and failure will be reviewed in bridging between technical and business to develop a culture of security and sustainability of security considerations across enterprises.

The session will look at how language, perspective, and operational processes and procedures differ between technical and business areas. Differences in how people work and get things done vary based on the resource skillsets and engagement circumstances. Variances in motivation and reward structures—and how they influence engagements—will also be explored.

Dr. Fortier has over 30 years of executive and technical leadership experience in federal technology environment working for a number of government contractors such as E-Systems, Titan Corporation, Intermetrics, and Cigital. He has conducted research in information systems security over the past 20 years. He was awarded a Research Fellowship at the George Washington University School of Engineering and Applied Science and the Institute of Crisis, Disaster and Risk Management (ICDRM). He currently is the associate director of ICDRM. Dr. also teaches part time in the Department of Engineering Management and Systems Engineering. He currently consults with the U.S. Government and Northcross Group providing technical solutions for challenging business and engineering problems. Dr. Fortier was granted a Doctor of Science (D.Sc.) from George Washington University; M.S., Information Systems, George Mason University; and M.S., Safety Studies, West Virginia University.

4:40 pm	**Door Prize Drawing – Green Auditorium** **Dinner Get Together – Location TBD *(Dinner is not included in the registration fee.)*** **Sign up at conference at the registration desk.**

Wednesday, March 25, 2015

Green Auditorium	**Welcome Announcements: Pat Toth, NIST** **Door Prize Drawing** **Vendor and Federal Agency Exhibition Preview Slide Show** **Poster Hallway – Open 10:00 am – 2:40 pm**

CISO Panel: Training & Education for the Security Leaders of Tomorrow

Carl Willis-Ford, SRA International, Inc., Moderator
Stephen Battista, ISSA-NOVA President, The MITRE Corporation
Dr. Jean-Pierre Auffret, George Mason School of Business
Derek A. Smith, Excelsior

What training/education/experience does it take to be an effective CISO? Cybersecurity covers such a broad spectrum: computer forensics, continuous monitoring, network traffic analysis, risk management, policy & governance, malware analysis…does a CISO need a well-rounded cybersecurity background or will deep expertise in any area suffice? Or…is a cybersecurity background even needed? This panel will discuss these questions from various viewpoints, exploring what training & education it takes to be a CISO.

Mr. Stephen Battista is a cyber security expert at The MITRE Corporation. He works in the Strategy, Policy and Privacy department in MITRE's Cyber Security Technical Center. He leads both a group of Cyber Security Engineers and MITRE's Cyber Security Corporate Intern Program. His areas of interest are corporate board oversight of cyber security, cyber security strategy, supervisory control and data acquisition (SCADA) security and machine learning in adversarial environments. With almost 25 years of practical and research experience in cyber security, he advises MITRE's sponsors on both research and operations to help secure their systems. He is the President of the Northern Virginia chapter of the Information Systems Security Association, a member of the Project Management Institute and holds both a Certified Information Systems Security Professional (CISSP) and a Project Management Professional (PMP) certification. Steve holds a BS and MS in Computer Science from Villanova University and a M.B.A. in Marketing from Temple University.
President, ISSA - Northern Virginia Chapter

Dr. Jean-Pierre Auffret is director of the executive degree programs in the George Mason School of Business including the MS in Technology Management, which is one of seven partners in the U.S. government's CIO University; the MS in Management of Secure Information Systems, which is jointly offered by Mason's School of Business, Volgenau School of Engineering and School of Public Policy; and the Executive MBA.

He is a co-founder of the International Academy of CIO and serves as an advisory board member of the Waseda eGovernance Research Center. Auffret's academic experience includes teaching at the Duke University's Duke Center for International Development, American University's Department of Physics, American University's Kogod School of Business, and the University of Maryland Robert H. Smith School of Business.

Auffret has served on several recent Commonwealth of Virginia commissions and committees including the Commonwealth of Virginia Health Information Technology Advisory Commission (HITAC) and the Electronic Medical Records Advisory Committee of the Virginia General Assembly's Joint Commission on Technology and Science (JCOTS). He has 30 years of technology industry and academic experience including management and executive positions with MCI and its joint venture with British Telecom, Concert.

Derek A. Smith is responsible for the development and coordination of cybersecurity initiatives at NCI. Formerly, he has worked for a number of IT companies including Computer Sciences Corporation and Booz Allen Hamilton. Derek spent 18 years as a special agent for various government agencies and the military. He has also taught business and IT courses at several universities for over 20 years. Derek has served in the US Navy, Air Force and Army for a total of 24 years. He completed an MBA, MS in IT Information Assurance, Masters in IT Project Management, and a B.S in Education. Derek is currently studying for a Doctorate of Business Administration degree in Organizational Leadership.

Pecha Kucha (Lightning Round) and Speak-Out

During Pecha Kucha (Lightning Round) speakers will 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, Potomac Forum

- Sandy Toner, ICF International
- Frank Cicio, Jr., iQ4 Corporation - " Transforming the Next Generation Workforce"

Speak-Out

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

Visit the Vendor and Federal Agency Exhibition in the Poster Hallway

- ***During the Morning Break 10:10 – 10:40***
- ***During the Lunch Break 11:50 – 1:15 (Note, DIACAP to RMF starts at 12:45)***
- ***During the Afternoon Break 2:25 – 2:45***

View the FISSEA Security Contest entries in the foyer area across from the Red Auditorium.

Level-Setting Security Training Material for Security Professional Dynamically

Kevin M. Stoffell, Cyber Security Architect, Battelle Memorial Institute

The use of appropriately detailed security training material is critical to capture audience attention and ensure the intended learning objectives are fully met for all participants. Overly detailed material for an audience will cause attendees without sufficiently deep basis for understanding the material to miss the learning objectives, while insufficiently detailed material will lose the interest of more advanced attendees.

This topic discussion covers several effective methods to level-set information security training materials and the presentation of materials for a particular intended audience. By creating an overall training or education package around a core theme and format, the package can be effectively utilized for a wide range of potential audiences through the use of modularization with supplemental and alternate material utilized for different audiences. By crafting the training package to include introductory through advanced material as an integrated package, modularization of package elements can be used to quickly customize the material for the appropriate level of detail to meet the training objectives for a particular audience. This approach also allows a course instructor significant flexibility to dynamically adjust the level of detail presented based on interactive feedback with training attendees.

Two methods for creating an integrated training package of this type will be discussed; one involves intentionally creating a modularized multi-audience package from the ground up, while the other involves modifying an existing package to increase its effective audience base.

A brief example of this approach utilizing a notional training package on the NIST SP 800-53 Controls will be included.

Mr. Stoffell is currently a Cyber Security Architect with the Cyber Architecture and Advisory Services division of the Cyber Innovation Unit at the Battelle Memorial Institute. He has over 18 years of experience in information systems operations and information systems security in academia, military, and commercial environments. Mr. Stoffell assists both Federal and commercial clients with the evaluation, design, and implementation of effective Cyber Security Architectures and the characterization of Cyber-related risk based on both specific and general threat scenarios.

Mr. Stoffell is an Authorized Instructor with the International Information Systems Security Certification Consortium $(ISC)^2$, teaching both Engineering and Management related certification training courses. He has achieved numerous professional certifications in information systems security, systems engineering, and project management. He has a Bachelor's of Science Degree in Computer Engineering from the University of South Carolina, and a Master's of Science Degree in Electrical Engineering from the Naval Postgraduate School.

SIFMA Members to Join the CUNY Workforce Alliance … Tackling Cybersecurity Skills Shortages

Frank C. Cicio Jr., Chief Executive Officer / Founder, iQ4 Corporation

"Transforming the Next Generation Workforce" was presented during Pecha Kucha and this presentation is the use cases. iQ4, SIFMA members, the City University of NY (CUNY) and NYU have teamed to form a digital workforce development alliance, to address the significant lack of qualified Tech Risk (i.e. cybersecurity, business resilience, risk governance) resources with industry knowledge, by bringing the Financial and Healthcare Industry world and education together to define a common set of skill/knowledge requirements and use cases that can be used in creating a scalable virtual project curriculum. The initial launch will be with CUNY and NYU/Poly, with the objective of making the expectations scalable to any academic institution. Tech RISK represents a critical market skills gap and involves disciplines and resources across campus including degrees in STEM, business, marketing, accounting, law and liberal arts.

Following our success with NASA, the key to this program is linking industry, government and their current and future Tech RISK workforce needs to universities to develop the technical competencies to build, operate and defend enterprise systems delivering critical financial and infrastructure services.

CUNY's Vice-Chancellor's office of Student Affairs will be leading this collective effort. With a community of 450,000 students and 24 colleges, CUNY seeks to extend its national leadership role in providing global talent. The CWA effort launches with three objectives:

1. Aligning education to meet industry skills and certification requirements in Tech RISK
2. Student Awareness and Development of skills using Industry Frameworks (e.g. NICE)
3. Experience – Fashioning seamless business participation using a cross-community workforce and a development skilling platform to enable "virtual real-world internships"

Frank C. Cicio Jr. is CEO and Founder of iQ4 LLC. iQ4 is dedicated to solving the challenge of student employability, workplace skills development and transforming the next generation workforce. Prior to starting iQ4 in 2007 Frank has served as an emerging technology executive for 35 years taking two start-up companies public, one start-up acquisition and one turnaround company acquisition. These results were inspired through world class team building and entrepreneurship, leading to the transformation of high growth private businesses into public market leaders. Frank's brings a broad experience to his business building background including funding and maximizing shareholder equity.

Frank is an industry thought leader and evangelist speaking in boutique as well as major industry forums, his organizations have been recognized globally, winning dozens of awards and serves on various boards including NYU Poly Advisory Board, ITiB President and venture partner with InSight Capital Partners.

Frank has a Bachelor of Science Degree in Marketing from Manhattan College and post-graduate work at both Princeton and the University of Pennsylvania's Wharton School of Business. He has two teenage boys, a wonderful and supportive wife, coached soccer for ten years, jazz and blues keyboardist, avid tennis, skier and fisherman.

Growing a Cybersecurity Team: How Collaboration Within an Organization is Changing

Michael Petock, Subject Matter Expert and Training Developer, Information Assurance Branch, US Department of State, Diplomatic Security (DS/SECD/IAB)

Presentation addressing challenges in government space, particularly with Growing a Cybersecurity Team: How Collaboration Within an Organization is Changing. Since the original concept ideas of safeguarding information, those assigned the responsibilities for information security has changed and are continuing to grow. Our organizations must recognize that growth by identifying all the team members and train them to successfully complete their responsibilities. This presentation will discuss and identify old and new security team members and some of the offerings to train them.

Desired Learning Outcomes: Enhanced staff awareness throughout an organization of those not formally designated with cybersecurity responsibilities yet still support cybersecurity protocol implementation.

Michael Petock has supported the U.S. Department of State's information assurance training program as a trainer and Subject Matter Expert, since 2002. 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 Information System Security Line-of-Business program, Mike has supported enterprise information assurance training programs with DHS, SSA, FBI, and NARA.

The courses Mike designs focus on involving the audience in the learning process. This session will provide audience members an opportunity to experience a very powerful activity that will help identify some of the agency's security professionals and their responsibilities. He will also lead discussions on some of the "hidden" roles that need to training in order to support security in the life cycle of a system.

Training Organizations to Prevent Cyber Attacks

Dr. Matthew McFadden, Manager and Lead Architect / Engineer, Computer Sciences Corporation

Note: Slides may not be posted.

Hand's on practical application is the most effective way for an organization to train against cyber threats. Whether you are an information security officer, a seasoned system administrator, or a non-technical individual seeing and experiencing a cyber attack drastically increases awareness and detection. This presentation demonstrates a few different attacks and how you can best "show" your organization how to prevent a serious intrusion.

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

Visit the Vendor and Federal Agency Exhibition during the lunch break

Practical Awareness Program

Eugene Taylashev, Nellie MacNeil; IFDS Canada

This presentation covers practical and layered approach for Information Security education and awareness in an ISO 27001:2013 certified organization. Will be discussed security policies and attestation, elements of the education program and enforcement, simulated phishing attacks and key performance measurements.

Eugene Taylashev is experienced with challenges and opportunities in the areas of IT Governance, Information Security and risk management with more than 20 years of hand-on experience. Worked for industry-leading firms such as PricewaterhouseCoopers and Deloitte. Managed and conducted SAS70 / CICA 5970 / SSAE 16 / CSAE 3416 / SOC 2 and risk based IT audits for many organizations in different industries. Recently implemented Information Security Management System (ISMS) and managed ISO 27001 certification for IFDS Canada. Certification: CISM, CCNA, MCSE. LinkedIN: http://ca.linkedin.com/pub/eugene-taylashev/28/b5/812

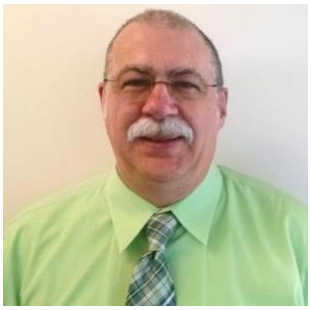
Nellie MacNeil is a Sr. Information Security Analyst with IFDS Canada. She is experienced in all aspects of InfoSec education and awareness as well as IT Audit and ISO 27001 certification. She has more than 10 years of hands-on Information Security experience.

DIACAP to RMF Conversion

Marc E. St. Pierre, CISSP - M.S. Network Security, Enterprise Information Assurance Manager, emagine it

The recent Government mandate to convert from DIACAP to Risk Management Framework (RMF) has caused unnecessary delays in certifying programs. The root cause is a variety of uncommon approaches in conveying what programs currently have into RMF. To better understand and integrate current package into RMF a new approach to conversion is required for clarity into the DOD requirements. The RMF conversion is not difficult once the basics of Configuration Management and Audit are properly applied to the program CONOPS. Substantial progress was made in the SP800-53 Rev4 that provides a continuous flow for all Information Assurance requirements. I wish to explain the benefits and coordination required via Areas of Responsibility (AOR), Team configuration and

Control Overlap to complete this conversion in a timely manner. Careful planning and training can reduce the completion time and make the Continuous Monitoring model work more efficiently.



Marc E. St. Pierre - 26 years' IT related experience and 8+ years IA/Security experience. Graduate of Capitol College received an MS Network Security 2005, GPA 4.0. CISSP, since 2007. In 2012 awarded a Self-Certification ATO from DSS for a contiguous single System Security Plan developed to cover the IA requirements of multiple cognizant authorities. (DIACAP/NIST/NISPOM/DCID/JFAN). 2009 Air Force project efforts resulted in reduction of ST&E and C&A time required for completion from 2 weeks to 2 days using Six Sigma Processes. Managed a Six Sigma project which consolidated software support efforts for year 2004 and resulted in a 43% savings (slightly over $120,000.00) in yearly maintenance renewal costs over the remainder on the project.

Keys to Employee Cybersecurity

Al Lewis, CISSP, CISM, Cyber Security Policy & Compliance Lead, MITRE Corporation

An engaged user – one who is educated and aware about cyber threats and their role in responding to them – is the best defense against cyber threats for any organization. There are a few simple, fundamental truths that exist in cyber security education, training, and awareness – and these truths have existed from the founding days of FISSEA to today. Come and share a look back in time from where our field has been to where we may be going – as this speaker shares his thoughts about best practices in educating, informing, and engaging users to help protect data and systems.

Albert (Al) Lewis, Cyber Security Policy & Compliance Lead for the MITRE Corporation, possesses over 20 years of progressive leadership experience in cyber security engineering, policy, governance, and compliance. Mr. Lewis helped to create the Computer Security Incident Response Team/Security Operations Center for a critical DoD global network immediately following 9/11. He has served the FBI, Department of Energy, U.S. Supreme Court, and numerous other federal agencies in helping to create enterprise risk management policies and practices, and has created and chaired risk governance committees to institute these policies and practices. At MITRE, he serves the CSO and CISO by managing all governance, policy, and compliance initiatives for the corporation. Mr. Lewis earned his MS in Information and Telecommunication Systems from Johns Hopkins University. In 2009-2010, he participated in the ASIS/Wharton Business School program for security executives. He also holds the following industry certifications: CISSP-ISSMP, CISM, CGEIT, FITSP-M, NSA IAM, and NSA IEM. He is a member of FBI InfraGard.

Preparing Future Cybersecurity Leaders

Derek A. Smith, Director of Cybersecurity Initiatives, National Cybersecurity Institute (NCI) at Excelsior College

The topic of most discussions on cyber workforce development centers on the need to develop skilled cybersecurity professionals to meet the growing demand. However, there is an equal need for the development of highly skilled cybersecurity leaders, such as Chief Information Security Officers (CISO). While colleges and universities have developed programs to educate cybersecurity professionals in the knowledge, skills and values required to work in their field, these programs are not preparing the next generation of Cybersecurity leaders for top cyber leadership positions.

Cybersecurity managers must possess the skill to design and implement strategies to deal with difficult cyber threats. However, they must also understand the business aspects of their job. Few university programs or training programs are designed specifically to prepare the next generation of CISOs in the critical business skills they require.

This presentation will:

1. Discuss why organizations should implement and refine the CISO role and why this role must have the same level of importance as other “C” level roles.
2. Discuss what educational institutions should do to build leaders well versed in both technology and business skills.
3. Discuss key abilities that future CISOs should develop in preparation for this role.
4. Share findings from our national CISO survey.

Derek A. Smith is responsible for the development and coordination of cybersecurity initiatives at NCI. Formerly, he has worked for a number of IT companies including Computer Sciences Corporation and Booz Allen Hamilton. Derek spent 18 years as a special agent for various government agencies and the military. He has also taught business and IT courses at several universities for over 20 years. Derek has served in the US Navy, Air Force and Army for a total of 24 years. He completed an MBA, MS in IT Information Assurance, Masters in IT Project Management, and a B.S in Education. Derek is currently studying for a Doctorate of Business Administration degree in Organizational Leadership.

Visit the Vendor and Federal Agency Exhibition during the afternoon break

Perspectives on Augmenting Federal FISMA Practices with Cybersecurity Framework – Panel

Matthew Barrett, Program Manager, NIST Cybersecurity Framework, NIST;
Kelley L. Dempsey, Senior Information Security Specialist, Information Technology Laboratory/Computer Security Division, NIST;
Vinny Troia, CEO, Principal Security Consultant, Night Lion Security

The NIST suite of FISMA guidance continues to provide a comprehensive set of information risk management approaches, methodologies, and practices that are required for Federal agencies and often adopted based upon business value within private sector. The recently published Cybersecurity Framework to Improve Critical Infrastructure Cybersecurity (Executive Order 13636) was chartered as a voluntary guidance for critical infrastructure, and may have business value for Federal use. This panel will explore ways in which Federal agencies can augment their FISMA-based risk management and risk management education efforts, with the Cybersecurity Framework.

Matthew Barrett, Program Manager, NIST Cybersecurity Framework
Mr. Barrett and his team are responsible for establishing and maintaining relationships with both private and public sector Cybersecurity Framework stakeholders. Mr. Barrett works through those relationships to provide perspective and guidance, as well as gather input on use of the Framework and to inform broader NIST cybersecurity activities.

Matt is also known for his program management of the Security Content Automation Protocol (SCAP) Program and NIST's support of OMB's Federal Desktop Core Configuration initiative (predecessor to the U.S. Government Consensus Baseline initiative). Previous to NIST and over the past decade, Matt has served in various IT security executive roles.

Kelley Dempsey began her career in IT in 1986 as an electronics technician repairing computer hardware before moving on to system administration and network management. While with the Department of the Navy in 1998, she began focusing on information system security and conducted a large scale DITSCAP certification and accreditation from start to finish. In 2001, Kelley joined the NIST operational Information Security team, managing the NIST information system certification and accreditation program and then joined the NIST Computer Security Division FISMA team in October 2008. Kelley has co-authored NIST SP 800-128 (Security-Focused Configuration Management), NIST SP 800-137 (Information Security Continuous Monitoring), NISTIR 8011 (Automating Ongoing Assessments), and NISTIR 8023 (Risk Management for Replication Devices), and is a major contributor to NIST SPs 800-30 Rev 1, 800-37 Rev 1, 800-53 Rev 3/Rev 4, 800-53A Rev 1/Rev 4, 800-39, 800-160, and 800-171. Kelley earned a B.S. in Management of Technical Operations, graduating cum laude in December 2003, and an M.S. in Information Security and Assurance in December 2014. Kelley also earned a CISSP certification in June 2004, a CAP certification in January 2013, and a Certified Ethical Hacker certification in November 2013.

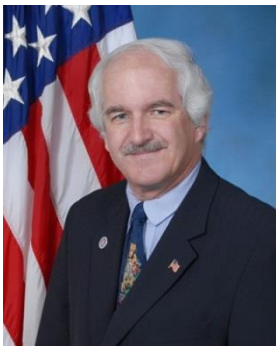
CEO of Night Lion Security, Vinny Troia has 18+ years of IT security and software development experience, and is nationally recognized as being an expert in cyber security and computer forensics. About 8 years ago, Troia shifted focus and began working on Military and Department of Defense projects. Troia has significant experience leading, architecting, and implementing secure website and network security solutions for both commercial and Federal organizations. Troia also understands the intricacies of Federal information security, which is what initially caught the attention of the national TV media. Troia is regularly featured as a guest on major news networks such as CNBC, Fox, ABC and CNN, and is currently pursuing a PhD in Information Security from Capella University.

Defending Our Nation in Cyberspace

Craig Holcomb, Senior Computer Scientist, National Security Agency

How are you protecting yourself from thieves in Cyberspace? How are we as a nation and country protecting ourselves from threats in Cyberspace? If you combine protection and defense this defines itself as CyberSecurity. This unique presentation provides a view of cybersecurity and its threats such as infected websites, infected emails, phishing attacks and social engineering from a national level down to the home user, and presents how it takes a team to make Cyberspace more secure. The talk provides "homework time" on how to secure your home computer via a variety of "tasks."

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



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

Army Reserve Cyber Private Public Partnership

Lieutenant Colonel Scott Nelson
Office of the Chief of the Army Reserve, Private Public Partnership Office, Cyber Security Branch

USAR is growing its Cyber Force and to meet the demand of the Army. We are partnering with Academia and Industry to recruit, develop and retain critical cyber skills in our force. The USAR is unique in its ability to link military and civilian skills for cyber. When integrated into a structured program like Cyber P3i supporting our Cyber units and linked with USCC training requirements we believe we can muster a force sought by ARCYBER and USCC. Cyber P3i is designed to meet current and future cyber requirements for the USAR, Army and Joint Force. Matching academic, employer and community outreach networks with Cyber operations and force development. Cyber P3i aims to support USAR Individual, Leader and Unit readiness for the Cyber Force. This includes soldiers conducting Cyber Defense, Network Operations, cyber resilience and systems deployment. It will also develop our leaders to understand, prioritize and integrate cyber into their training and operations.

- Individual Readiness: Recruit/Develop/Retain USAR Cyber Force
- Leader Readiness: Enable Leaders Cyber understanding
- Unit Readiness: Enhance Operational readiness

Cyber P3i is designed to be a regionally focused, nation-wide program aimed at national cyber innovations centers with a skilled cyber population, USAR cyber soldiers and units. Regions include: NE, SE, SW, West, Rocky Mountain and Central. To date we have 6 Universities signed up for the partnership, with over 10 standing by to partner with the USAR. This is good for the Army and Joint Cyber Force as it provide the operational bench to meet Strategic, operational and tactical cyber force demands. This initiative provides opportunities to retain critical cyber skilled AC soldiers (the Army's Cyber investment) by transitioning them to the USAR and Civilian careers.

Cyber P3i Endstate: USAR Cyber force soldiers are educated through Army, Joint and Higher Education developing critical technical and thinking skills to react to dynamic cyber defense. Cyber AC transitioning soldiers see the USAR as military organization of choice. USAR and Army recruiting is meeting demands of Cyber force (currently middle and high school students). USAR Cyber force is in continuous learning process through employment with industry/government, higher education programs with partner Universities and linking military and civilian cyber skills to meet Army Cyber force requirements. The Army sees the USAR Cyber force as critical to its success and the USAR cyber is fully integrated operationally into the Army.

Lieutenant Colonel Scott Nelson is the Program Manager of the USAR Cyber Private Public Partnership Program. He also currently Commands the Army Reserve Element at US Special Operations Command. His past position was as the Deputy Commanding Officer for the US Army Reserve Cyber Operations Group, Adelphi, Maryland. He served as the Commander of the North American Aerospace Defense Command (NORAD) and US Northern Command (USNORTHCOM) Army Reserve Element (ARE) and IO Section Chief/IO Intelligence Officer for the NORAD/USNORTHCOM J39 Information Operations Division. In this role he supports NORTHCOM missions in Homeland Defense, DSCA and Security Cooperation including multiple events with building MEXMIL IO capacity. He is native of Richland, Washington and a graduate of the University of Montana (Bachelor of Science in Business, 1991).

He was commissioned a 2nd Lieutenant after completing ROTC on 27 November 1990. He currently was selected for the Army War College DDE program.

His awards and decorations include the Bronze Star, Defense Meritorious Service Medal, Army Meritorious Service 4OLC, Joint Service Commendation, Army Commendation 5OLC, Joint Service Achievement, Army Achievement, Armed Forces Expeditionary, Armed Forces Service, NATO Medal (2), Army Reserve Components Achievement, Armed Forces Reserve, Afghan Campaign Ribbon, Global War on Terrorism Expeditionary and Service, Humanitarian Service and National Defense Service Medals. LTC Nelson has earned the Overseas, Army Service, and Army Reserve Overseas Training Ribbons.

As a military officer LTC Nelson has also served as an Army IO Instructor, IO staff officer for National Guard Bureau and Department of Army Mobilization, Operations Information Operations Directorate (DAMO-ODI), lectured at the Army War College on Strategic Communications, served as a Legislative and Congressional Affairs Officer and previously served as a program manager for the development of doctrine, training, force structure and leader development for the Army Theater Information Operations Groups and ARNG Cyber units.

Information Assurance as a College Major

Sherry Lakes, Doctor of Science, Capitol Technology University

Burch (2011) reported a significant increase in cyber-attacks in the United States over the last several years. Although this increase in cyber-attacks has also increased the demand for cybersecurity professionals, a significant number of cybersecurity-related positions in U.S. organizations are going unmet. In response to the U.S. cybersecurity workforce shortage, NICE has proposed on-going national strategies to include raising awareness about risk in cyberspace, broadening the pool of individuals prepared to enter the cybersecurity workforce, and cultivating a globally competitive cybersecurity workforce (McDuffie, et al., 2013). Although applicable educational/training programs are imperative for the success of these strategies, Andress and Winterfield (2011) have suggested that educational programs focusing on cybersecurity at institutes of higher learning are still in their infancy. Establishing and implementing relative educational programs require that organizations understand the discipline and the factors that motivate students' interest in that discipline (Darling-Hammond & Baratz-Snowden, 2005).

Dr. Sherry Lakes has 35 years of diverse experience in executive and technical positions. She has been responsible for the overall strategic direction and management of multiple organizations. Equally, her technical roles have required her developing and fielding solutions and systems across a diverse set of problem domains. Dr. Lakes' professional credentials include Project Management Professional (PMP) and Certified Information System Security Professional (CISSP-ISSEP) certifications.

She frequently consults for advisory boards of education organizations and recognizes the need for government, industry, and academia to partner on STEM initiatives. She also recognizes the role of STEM on the nation's economy and security, and on present and future career opportunities. As such, her goal is to share the experiences and knowledge she has attained, thus helping to prepare students of all backgrounds for success.

Sherry holds a Doctorate Degree in Cybersecurity from Capitol Technology University, a Graduate Degree in Management of Information Systems from Bowie State University, and a Bachelor's Degree in Business Management from Washington Adventist College.

A native of North Carolina, Dr. Lakes enjoys traveling with her husband and daughter.

Evaluating the Security Implications of Innovation, Risk, and Risk Reduction in the Internet of Everything - Panel

Valorie J. King, PhD, Collegiate Associate Professor;
Samuel Chun, Assistant Professor (adjunct);
Richard White, PhD, Adjunct Associate Professor; University of Maryland University College, Computer Information Systems and Technology Department

Cybersecurity professionals need to be prepared to evaluate the security implications of leading and emerging technologies, both good and bad. In this panel discussion, three UMUC faculty members will present our scenario-based approach to preparing cybersecurity professionals to identify and then objectively evaluate the security implications of technology innovations which have the potential to impact risk and risk reduction in the Internet of Everything. The evaluation methodologies used in our courses include: Analysis of Alternatives, Case Studies, Delphi Method Studies, Experiments and Quasi-Experiments, Gap Analyses, Pilot Studies and Implementations, and Product Assurance Evaluations.

Our starting point will be a discussion of our experiences using a series of scenario-based assignments in which students are asked to identify one or more technologies which are on the verge of exiting the research & development lab or an emerging application of existing technologies which has resulted in the creation of new products or services. These assignments include researching the characteristics of a selected technology and how it is likely to be used in designs for new products or components which will eventually make their way into the Internet of Everything as computers, digital devices, and other electronic / electrical technologies (this includes networks and network infrastructures).The assignments also include the design of formal evaluation studies in which potential or reasonably anticipated security issues and concerns will be identified and assessed. The evaluation studies were required to address, at a minimum, the following research questions:

- How can this technology or emerging application of technology be used to improve or support the security of devices and services which comprise the Internet of Everything?
- How can this technology be used by attackers, criminals, terrorists, etc. to achieve their goals and objectives within the context of the Internet of Everything?

Dr. Valorie J. King has taught information security and information systems management since 2006. Currently, she is a Collegiate

Associate Professor and Course Chair for the Cybersecurity (CISA) program in The Undergraduate School at the University of Maryland University College. In addition to teaching the technical, management, and policy aspects of cybersecurity, Dr. King is involved in designing courses and creating curriculum materials for the Cybersecurity Policy and Management major and the Digital Forensics track of the Computer Networks & Cybersecurity major. She also serves as a course chair for in both areas. Dr. King's practitioner experience includes serving as a Deputy Division Chief (Information Assurance Systems and Software) and as a Department of Defense Office of the CIO Senior IT Policy Analyst (Web policy / E-Gov). Her IT consulting engagements have included serving as an IT Strategist, IT Policy Analyst, and Software Engineering subject matter expert for secure networks and systems. She has over fifteen years hands-on Software / Systems Engineering for mission critical systems in secure environments.

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

Mr. Samuel Chun is Vice President for Alliance Sales and WW Channels for HP Enterprise Services (HPES). He is responsible for the accelerated growth of HPES's global sell-with and sell-through business with their strategic partners and select channels. His theater of responsibility includes billions (USD) in joint selling with partners annually.

Previously, Mr. Chun was Vice President, World Wide Security Services Sales Leader for HP Enterprise Services. He led the alignment of key security assets within HP's service, product, and geographic business groups for driving the WW security service business for HPES. Before joining HPES's Global Sales organization he was the director of the Cybersecurity Practice for HP Enterprise Services U.S. Public Sector where he led the strategy, portfolio development and industry messaging of cybersecurity services and solutions for U.S. Public Sector clients.

Mr. Chun joined EDS, now HP, in 2008 from the joint program office of the Secure Information Sharing Architecture Alliance (SISA), a security consortium led by Microsoft, Cisco, and EMC for the global government market. Previously he was the director of information assurance for the Enterprise Technical Services Division of TechTeam Government Solutions (now Jacobs Technology) where he served for 10 years in a variety of internal and external security roles, including leading the company's compliance to the Sarbanes-Oxley Act of 2002.

Mr. Chun holds a variety of industry certifications, including being a Certified Information Systems Security Professional (CISSP). He is an industry authority on information security and a prolific writer having been published in nearly twenty books and periodicals. Chun is a regular speaker at industry conferences and cyber security policy workshops and recently provided expert testimony on the "State of Federal Information Security" at a hearing before the House Subcommittee on Government Management, Organization and Procurement.

Mr. Chun is also an Assistant Professor (adjunct) in Cybersecurity program at the University of Maryland University College and is a graduate of the Johns Hopkins University in Baltimore, Md., where he received both his bachelor's and master's degrees.

Dr. Richard White has taught data communications and computer security since 2001. As an Adjunct Professor, he started with UMUC in 2007 in the Information Systems Management program. In 2010 he moved to the Cybersecurity & Information Assurance program where he teaches multiple cybersecurity courses, as well as serves as the Course Chair for the CSIA capstone course - Practical Applications in Cybersecurity Management. In addition to teaching for UMUC he also serves as the Managing Director for Oxford Solutions. Prior to Oxford Solutions Dr. White was the Chief Information Security Officer for the

United States Capitol Police. Dr. White earned a PhD from Capella University and an MS from UMUC. Prior to his employment at the United States Capitol Police he provided systems engineering and information assurance consultation, through Booz Allen Hamilton, for the Intelligence Community, Department of Defense and civilian agencies of the federal government.

Did you know…. FISSEA holds an annual conference every March. Plan ahead for 2016.

FISSEA is a volunteer organization run by and for federal information systems security professionals with an interest in awareness, training, education, and certification. Vendors and contractors who work with and support federal IT security programs are also members, as are members of the academic community. FISSEA assists federal agencies in meeting their computer security training responsibilities.

Patricia Toth is Chairperson of the Working Group (WG) from various agencies and organizations. Peggy Himes has worked with FISSEA Executive Boards and Working Groups since 1998.

Thank you…..

- **Attendees. We hope you found our conference of value.**
- **Speakers for donating their time, energy, and knowledge.**
- FISSEA Technical Working Group for their input on the agenda and assisting with on-site details. Gretchen Morris for coordinating the Security contest. Sue Farrand for coordinating the prize donations.
- NIST Computer Security Division support:
  - Patricia Toth, Conference Chair
  - Peggy Himes following-up with speakers, preparing the agenda and conference program.
  - Judy Barnard for website updates and designing the program cover.
- American Public University for donating bags for all attendees.
- Prize drawing contributors: SANS, CompTIA and Partners, TVAR, Carl Willis-Ford, Al Lewis, Art Chantker, and possibly more.
- NIST Public and Business Affairs: Mary Lou Norris, Gladys Arrisueno, Teresa Vicente, Crissy Robinson
- The Federal Business Council: Liz Hood, Tina Sheehy, George Hall, and Rachel Tedesco.

FISSEA Working Group	
Scott Anderson, Veterans Affairs (VA) Dan Benjamin, American Public University Terry Brox Art Chantker, Potomac Forum Terri Cinnamon, VA Brenda Ellis, NASA Susan Farrand, Dept of Energy Raymond Greenlaw, USNA Angela Guinn, VA Susan Hansche, DHS Peggy Himes, NIST Lewis Craig Holcomb, NSA John Ippolito, Allied Technology Group	Lance Kelson, Dept of the Interior Sean Kern, National Defense University Albert Lewis, The MITRE Corp Gretchen Morris, DB Consulting/NASA Louis Numkin, FISSEA Life Member (retired IRS) Loyce Pailen, UMUC Davina Pruitt-Mentle, Cyberwatch Cheryl Seaman, National Institutes of Health Pat Toth, NIST, Chairperson Jim Wiggins, Federal IT Security Institute Dr. Kenneth L Williams, Army Carl Willis-Ford, SRA International Mark Wilson, FISSEA Life Member (retired NIST)