30th fissea
Securing the Future to Infinity and Beyond: Improving Cybersecurity through Awareness, Training, and Education
Federal Information Systems Security Educators' Association
March 14-15, 2017

2017 CONFERENCE PROGRAM

Presentations (receiving 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 14, 2017

Conference Welcome
Clarence Williams, NIST, FISSEA Conference Chair

Clarence Williams is the Government Engagement Lead supporting the National Initiative for Cybersecurity Education (NICE). Within this role he collaborates with governmental agencies and supports initiatives focusing on cybersecurity education, training, awareness, and workforce development. Previously, Clarence worked for Immigration and Customs Enforcement (ICE) within the Department of Homeland Security. He was a Regional Information Assurance Manager supporting the Office of the Chief Information Officer.

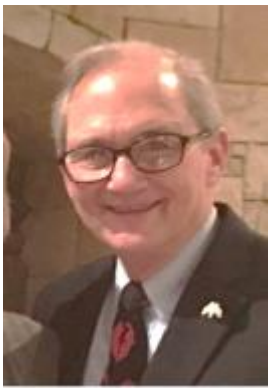
Before taking the position at ICE, Clarence worked with the Department of the Navy (DoN), in which he was a civilian system administrator (SA), trainer, and auditor of Public Key Infrastructure (PKI). Within this capacity, he was the lead SA over multiple sites, worked with the Information Systems Security Officer for system updates, created and delivered PKI training presentations to Navy personnel, and audited both ship and shore commands for compliance. Prior to this position, Clarence worked as contractor for the Department of Justice providing Tier 1, Tier 2, and Tier 3 support. He also provided technical support to several political offices on Capitol Hill, such as maintaining Correspondence Management Systems.

Clarence graduated from Campbell University in North Carolina with a BBA in Computer Information Systems, and received both his Masters of Science in Information Technology/Cyber Security Policy and Law from the University of Maryland University College.

NIST Welcome
Kevin Stine, Chief, Applied Cybersecurity Division, ITL, NIST

Kevin Stine is the Chief of the Applied Cybersecurity Division in the National Institute of Standards and Technology's Information Technology Laboratory. In this capacity, he leads NIST collaborations with industry, academia, and government on the practical implementation of cybersecurity and privacy through outreach and effective application of standards and best practices. The Applied Cybersecurity Division develops cybersecurity guidelines, tools, and reference architectures in diverse areas such as public safety communications; health information technology; smart grid, cyber physical, and industrial control systems; and programs focused on cybersecurity outreach to small businesses and federal agencies. The Division is home to several priority national programs including the National Cybersecurity Center of Excellence (NCCoE), the National Strategy for Trusted Identities in Cyberspace (NSTIC), and the National Initiative for Cybersecurity Education (NICE). Recently, he led NIST's efforts to develop the Framework for Reducing Cybersecurity Risk to Critical Infrastructure (Cybersecurity Framework) as directed in Executive Order 13636.

History of FISSEA
Louis Numkin, FISSEA Lifetime Member



Louis M Numkin, Educator or the Year and our first FISSEA Life Member:
"The first computer which I operated was an IBM 360-25 in 1969 which used DOS (Disk Operating System) with a card reader, twin tape drives, and a paper tape control for printer pagination. The room was very cold and we wore warm coats year-round while fixing the key punch or running a sorter when a deck fell on the floor. One of my first tasks was wiring boards for the reproducer and accounting machines while deciphering chad holes in IBM cards with the aid of an interpreter machine that looked like a drill press and only handled up to 60 of the 80-columns of Hollerith code at a time. Since my bits and bytes beginning, the IT world has changed and since retirement a few years ago, I have become just another user – doing no creation or modification of the laptop or its software which though only weighing a pound or two can do more functions at lightning speed when compared to my first computer. Of course, I still have my Timex Sinclairs which were the first advertised under-$100 computers sold to everyday citizens along with its cassette tape storage and gun-matrix thermal strip printer which included a primitive word processor, though it just gathers dust on a shelf over my desk. So, the times have changed and now we'll recount some of FISSEA's history for our attendees."

Keynote: Updates on Federal Cybersecurity from OMB
Grant Schneider, Acting Federal CISO, Office of Management and Budget (OMB)

Grant Schneider is the Acting Federal Chief Information Security Officer within the Office of Management and Budget, Grant Schneider leads a team of professionals who are responsible for enhancing Federal Government cybersecurity. This is accomplished through the establishment of strategy, development of policies and oversight of agency cybersecurity programs. Prior to joining OMB, Mr. Schneider served as Director of Cybersecurity Policy on the National Security Council and as the Chief Information Officer of the Defense Intelligence Agency.

Blunting the Phisher's Spear – Federal Phishing Programs That Work
Deborah Coleman, U.S. Department of Education;
Toney Rogers, Cybersecurity Training, Awareness and Education Lead, U.S. Department of Health and Human Services;
Kevin Sanchez-Cherry, DOT Cybersecurity Policy, Architecture & Training Lead U.S. Department of Transportation;
Peter Sindt, Section Chief Cyber Security Awareness and Outreach, Transportation Security Administration, U.S. Department of Homeland Security;
Karen Urban, Information Systems Security Manager, K2Share, Moderator

Email is the most direct route to personnel within Federal agencies, from the Secretary to janitorial staff. Armed with this knowledge, criminal groups, hackers, foreign nations, and others with malicious intent are using increasingly sophisticated malware and social engineering techniques to target Federal personnel with email-borne attacks and gain access to sensitive systems and information behind agency firewalls. As technology alone cannot prevent these attacks, end user awareness must be enhanced. Simulated phishing programs are a great way to accomplish that goal. Creating, maintaining, and measuring the effectiveness of phishing programs can be challenging, especially in a Federal agency with offices and end users across the Nation. This panel presentation offers approaches and solutions successfully used to overcome those challenges. Panelists from several agencies will share how they stopped feeling frustrated, learned to leverage agency culture and politics to gain buy-in for their programs, produced successful phishing campaigns that strengthened awareness and accountability at the human layer, identified metrics to measure the effectiveness of their programs, and reduced agency risk by blunting the phisher's spear.

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 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.

Toney Rogers currently serves as the Cybersecurity Training, Awareness, and Education Lead for the Department of Health and Human Services (HHS). As the Lead, Toney managed the deployment and ongoing operations of the HHS Ethical Phishing program consisting of more than 100,000 users across 12 independent Operating Divisions. He also leads the Department's Cybersecurity Training, Awareness, and Education initiatives and working group.

Prior to HHS, Toney spent 12 years at the International City/County Management Association Retirement Corporation (ICMA-RC) where he worked to create the first website designed to automate the retirement plan rollover process and a proprietary customer relationship management system ultimately preserving more than 50 million in assets for ICMA-RC.

Mr. Rogers holds a Bachelors of Arts degree in Economics from The Ohio State University and a Master of Cybersecurity Policy from the University of Maryland, University College.

Kevin Sanchez-Cherry is the Cybersecurity Policy, Architecture and Training Lead for the US Department of Transportation's (DOT) Office of Cybersecurity and Information Assurance, serving as the Program Manager for the Department's Cybersecurity Policy, Training & Education, and Cybersecurity Workforce Management Programs. In this capacity, Kevin has led the creation, development and implementation of the DOT Cybersecurity Workforce Management Program and has revised the Cybersecurity Training & Education Program. He is also a senior advisor to the DOT Chief Information Security Officer (DOT CISO) on cybersecurity policy, training and workforce management.

Prior to joining DOT in 2014, Kevin served four years with the US. Department of Education's Office of Information Assurance Services (IAS), as IAS Governance Program Manager, Acting Policy and Planning Branch Chief and IAS Records Officer. He also served four years with the United States Secret Service as the Certification and Accreditation (C&A) Program Manager, where he was responsible for leading the Secret Service's C&A and ISSO Programs.

Prior to the Secret Service, Kevin served over eight years in a variety of information assurance and IT security positions for the US Department of Commerce, National Archives and Records Administration (NARA), Department of Justice Antitrust Division, Department of Veterans Affairs, Veterans Health Administration Office, the Department of Defense's Military Health System (MHS), and in the private sector for the FINRA (formerly the National Association of Securities Dealers) Corporate Information Security.

He is the Founder and Co-Chair of the ISIMC Information Assurance Policy Working Group (IAPWG). The IAPWG provides interagency coordination and cooperation in the development and maintenance of cybersecurity policies, standards and governance, as well as discusses current policy issues, shares experiences and information, and reviews federal cybersecurity laws, requirements, directives, and governance for agency implementation.

Peter Sindt is Team Lead for TSA's Cyber Security and Outreach section, brings a combination of technical cyber security and strategic vision to the Transportation Sector. For almost 15 years, Mr. Sindt has worked within the IT Security profession, improving cyber security programs within the Federal Government and assisting CIO's in the develop and implementation of strategic visions within their organization. Under the direction of the Executive Order for Cybersecurity, Mr. Sindt facilitates risk reduction efforts by partnering with industry to execute on national policy and provide strategic direction for the Transportation Sector. In addition to an external outreach initiative, Mr. Sindt heads an innovative cyber security training program for TSA's 65,000 employees, which focuses on behavioral changes and the promotion of healthy cyber habits both within their professional and personal lives.

TSA Slides will not be posted.

Karen Urban, Information Systems Security Manager at K2Share has over 25 years of experience managing, developing, and supporting a wide range of cyber security and education programs within the federal government and private industry. She is skilled in all aspects of the Security Authorization, risk assessment, security assessment, penetration testing, system auditing, incident response business continuity planning. She has served as an Information System Security Officer (ISSO) for numerous federal information systems and was selected as the Department of Homeland Security, Federal Emergency Management Agency's ISSO of the year in 2009. Ms. Urban leverages her cyber security expertise to develop educational strategies and programs that focus on reducing cyber risk and modifying user behavior. She currently leads teams within the Department of Education which provide cybersecurity and privacy awareness training, phishing program support, Cyber Risk Management Framework (CRMF) governance and assessment services. She is a member of InfraGard and currently holds a number of professional certifications including CISSP, CISA, CRISC, GPEN, GICSP, and PMP.

Two tracks from 10:50 to 11:50 – Green Auditorium and Portrait Room – Room location listed on the Agenda

Training Healthcare Executives on Developing Effective Cybersecurity Strategy

Dr. Calvin Nobles, Department of Defense (DoD) / U.S. Navy and Dr. William (Will) Triplett, Food and Drug Administration (FDA)

A growing concern for healthcare executives is the increasing sophistication of cyber attacks and nefarious cyber activities. From 2010 to 2014, the healthcare industry lost 37 million health records and invested 6 billion dollars to combat cyber attacks (WEDI, 2015). Cybersecurity vulnerabilities, threats, and attacks continue to plague the healthcare industry due to (a) the lack of IT investments, (b) poor security practices, (c) human error, and (d) hyperconnectivity and IoT. Researchers classify malevolent cyber activity as (a) data loss, (b) monetary theft, (c) attacks on medical devices, or (d) infrastructure attacks (Perakslis, 2014). Cyber-crimes enacted upon healthcare facilities range from private clinics, physicians' offices and large hospitals because healthcare is target rich due to (a) personally identifiable information, (b) patient medical data, and (c) financial transactions. The HIPAA imposes major charges, customarily after any significant data breach that encompasses Protected Health Information of patients, illustrating the need for cybersecurity strategy training. Cybersecurity is a business strategy that requires meticulous integration, implementation, and execution to hardened computer networks and infrastructure. Healthcare executives need training on developing effective cyber security strategies and defenses. As evident by the increasing number of cyber attacks, organizations struggle with developing a cybersecurity strategy. This presentation will provide insight on developing a cybersecurity strategy and defenses to address (a) risk, (b) threat intelligence, (c) network and infrastructure posture, (d) security training, (e) human factors, (f) CIO/CISO engagement, and (g) technology. Providing healthcare executives with cybersecurity strategy training will enable healthcare organizations to secure data and the network infrastructure.

Dr. Nobles is a Cryptologist in the U.S. Navy and currently assigned to Fleet Cyber Command. He is a department head that leads functional experts in cyber intelligence support. His professional work consists of leading and directing projects in cyberspace and intelligence operations, planning cyber operations, and ensuring information security. His research interests are technology implementation in cyber, cyber security threats, cyberspace operations, technological discontinuities, automation in cyber, and the adverse implications caused by technological deterministic thinking.

Dr. Triplett was hired into his current position within the Business Informatics Team (BIT) in a deputy capacity and is responsible for providing center-level oversight for innovative information management and digital government initiatives, executive sponsorship of center-sponsored IT projects, and strategic direction for the Food and Drug Administration Strategic Priorities. In this role, he serves as a senior advisor to the Director in matters related to developing and implementing strategic plans. He took the lead in developing the Center for Veterinary Medicine five (5) year FY 2016 – FY 2020 Information Technology Strategic Plan (ITSP) and CVM's one (1) year FY 2017 Information Technology Tactical Plan (ITTP). The IT Strategic Plan identified the IT priorities and provided a roadmap for closing the gap between its current and future IT needs.

Dr. Triplett also led the development of the CVM's Data Inventory and Open Data White Paper that sets goals and implements the Center's Initiative for sharing data with the public. The Open Data Initiative vision is to align CVM's organizational attitudes and objectives of achieving transparency with the public, as part of the Presidential Transparency Government Initiative. Prior to his current position, while on active duty at the National Naval Medical Center, he was responsible for leading the development of the medical center's business plan,

customizing data analytics dashboard, and implementation of electronic health records. He has shown leadership abilities in the series of positions held, with distinction, during his naval career, and in his civilian roles in the Department of Health and Human Services.

In addition, he currently serves as a member on the CIO Council, Scientific Computing Board, Data Standards Advisory Board, Open FDA Data Initiative Group, and other leadership organizations. He also retains a faculty appointment as an Adjunct Associate Professor in the Business Professional Program at University Maryland University College. Dr. Triplett received his Bachelor's Degree in Healthcare Management from Southern Illinois University, a Masters of Business Administration from Liberty University, and a Doctoral Degree in Strategic Leadership from Regent University.

How Organizations Can Use Big Data to Spot Security Superstars, Slackers, and Knowledge Gaps

John Findlay, Launchfire

Creating cyber security training programs that improve your organization's security posture is tricky. The first challenge is driving participation. Even if you're successful at getting people engaged, how do you know they're learning? And how do you know your program is changing behaviour? In this half fun, half nerd, session we'll examine how the combination of game-based learning and big data can help organizations implement training programs that make a difference. You'll learn how to design game-based programs that drive participation and generate relevant, surgical analytics to help you evaluate your program and its impact on your organization's security posture.

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.

Aligning COTS Training Models to Cyber Role-Based Training Requirement

Hillary N. Lewis, Chief, Information Security Branch, Senior Official for Privacy, Department of Health and Human Services (HHS) Office of Inspector General (OIG) and Mason Molesky, HHS OIG

HHS OIG has evaluated COTS vendors to identify training that meets the NIST 800-16 RBT requirements while providing meaningful, engaging material. There is a dearth of "out-of-the-box" training that is easily customizable and that also suits the needs of a federal cyber and privacy training and awareness program. OIG identified a vendor with modular offerings that appear to cover most, if not all, of the NIST 800-16 role categories and learning objectives. The project, which is currently underway, is mapping the roles and learning objectives in NIST 800-16 against the OIG roles and the modules in the COTS product. The presentation will present the challenge, outline the methodology and present progress in developing a modular, engaging cyber RBT program.

Hillary Lewis's background includes executive leadership in health IT and policy and leadership in privacy, security, data governance and IT systems management. As Senior Official for Privacy and Chief of the Information Security Branch at HHS OIG her role involves managing privacy and security risk for the IT infrastructure. This includes awareness and training activities for the enterprise: phishing, leveraging the FedVTE training opportunities, and developing new training materials to strengthen the first line of defense against the adversary – our people.

Mason Molesky is currently enrolled at the George Washington University in the Scholarship for Service Program. His work at OIG has included support for the roll-out of the eGRC and DHS CDM programs, development of animated shorts for Cybersecurity Awareness Month, and his work to map the NIST Role Based Training requirements against COTS products.

Ambassadors, Champions, & Security Partners!

Deana Elizondo, Sr. Manager, Cybersecurity Programs & Awareness, American Electric Power

• Security Ambassadors (Security resources assigned to a particular business unit or region; engaged in projects to design secure solutions, as well as lead education and awareness events.)

• Security Champions (Trusted business partners that are resources in the business unit, Operating Company, or region – they work with Ambassadors to understand Security initiatives and share with their business unit or region.)

• Security Partner of the Month Program (An opportunity to recognize individuals across the company who help advance AEP's Security mission to protect people, information, and assets.)

Deana Elizondo is the manager of the Cyber Security Programs & Awareness team within the Cyber Risk & Security Services organization at American Electric Power. She has been with AEP for 12 years and has spent the last 7 years managing this team. Deana's team is responsible for Enterprise Security Policies & Standards, Security Training & Awareness, Security Program & Project Management, and Change Management.

Prior to AEP, Deana worked at Huntington Bank for 17 years managing many different technical and operational teams. Her entrance into Security was managing a Treasury Management Technical Services group while at Huntington Bank, which included supporting critical systems such as Cash Vaults, Lockbox, ACH, and Wire Transfer.

Lunch – 11:50 – 12:55 pm

- We do not have lunch tickets this year.
- You can go through the cafeteria line, pay on your own, sit anywhere in the cafeteria or West Square.
- You can go off campus to a restaurant and return through any gate showing your Conference Badge and photo ID.

Visit the Vendor Expo in the Poster Hallway and see the FISSEA Security Contest Entries also in the Poster Hallway

- **New this Year! Vendors will be here both days.**

Presentation of FISSEA Security Contest Winners

By Gretchen Morris, Contest Coordinator

Award Certificates and slide show sharing all entries (more than any year prior):

- **10 Posters**
- **11 Videos**
- **04 Websites**
- **03 Motivational Items**
- **05 Newsletters**
- **10 Training Scenarios**

2016 FISSEA Educator of the Year Presentation

Presented by Gretchen Morris, 2015 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) 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 slide show on http://csrc.nist.gov/organizations/fissea/FISSEA-contest/previous-winners.shtml

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.

Surprise – the 2016 Educator of the Year is announced at the March 2017 Conference.

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

Susan Hansche, DHS, presented the FISSEA 2015 Educator of the Year Award to **Gretchen Morris, DB Consulting/NASA** on March 15, 2016. Gretchen's vast knowledge base, high work ethic, dedication to the improvement of information security awareness and training, and her commitment to coordinating the annual FISSEA Security Contest make her the perfect recipient for the award.

FISSEA Educator of the Year Award RECIPIENTS:

2016: Surprise – announcement made March 14, 2017
2015: Gretchen Morris, DB Consulting/NASA
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 from 2:05 to 4:40 – Green Auditorium and Portrait Room – Room location listed on the Agenda

Security Awareness Training, Yeah, I have a PowerPoint…

Marcia Mangold, Manager of Information Governance, Blue Cross Blue Shield of Michigan

Slides will not be posted.

Is your awareness training focused on meeting compliance requirements only? Did you know that awareness training has a lifecycle just like Governance or policies? Information Security is the focus of nearly every large organization. However, most programs consist of a yearly mandatory CBT or PowerPoint presentation that is based on a compliance or framework checklist, not on a strategically planned Information Security Awareness Training program. Today's ever-changing security landscape requires constant reinforcement. As an Information Security Awareness and Training manager for a healthcare insurer, I continuously advocate and promote additional IS awareness training above what is required by compliance. My high-level overview will focus on ways to turn your security awareness program into a repeatable evolving robust program.

Marcia Mangold is the Manager of Information Security Governance for Blue Cross Blue Shield of Michigan. An organization that delivers vital health care services to about 4.4 million Michigan residents and 1.3 million members outside of Michigan. Marcia has spent the past 17+ years using her abilities to be a business enabler for IT and IS and has worked for several multinational businesses, which include IBM and GE. Marcia focuses on awareness training and policy lifecycle management, which have brought recognition in the form of nominations for ISE (Information Security Executive) Awards for the BCBSM "Insider Threat (B-Secure)" and "InfoSec Training and Awareness" programs to her team and herself.

She earned her Bachelor of Science in Software Production and Management from The University of Detroit and a MSBIT (Masters of Science in Business Information Technology) from Walsh College of Business. Marcia is a Certified Information Systems Security Professional (CISSP), a founding board member of the local ISC2 chapter and a proud member of the Michigan InfraGard chapter, which is a partnership with the Cybersecurity branch of the FBI and private industries. In addition, Marcia's was a contributing NIST Big Data Public Working Group member for the NIST Special Publication 1500-4, *Big Data Interoperability Framework: Volume 4, Security and Privacy*, and her expertise in information security is quickly making her a recognized leader in the industry.

Marcia enjoys spending time with her family and volunteering. She is currently the director of the CERT team at her church. In her spare time, she enjoys felting, canning, fishing and winemaking.

Aligning Skills-based Training and Performance Assessments within Academia to Create a More Capable Federal Cybersecurity Workforce

Linda Montgomery, President, Cyber World Institute

The well documented world-wide cybersecurity skills shortage has organizations desperately seeking qualified workers who have the skills to perform their functional roles. Those enterprises, however, are impeded by education, training, and certifications programs that are knowledge-based only and lack the skills development and measurement required to produce an effective cybersecurity professional. This paradigm has resulted in a global skills deficit across the entire cybersecurity workforce. In order to meet the recommendations outlined in the National Initiative for Cybersecurity Education (NICE) and the NIST Cybersecurity Frameworks, academia and training organizations must develop cybersecurity professionals with the skills necessary to perform their jobs. This can only be accomplished by augmenting existing programs with skills-based training and performance assessments. This presentation will address a specific solution set that can be integrated in post-secondary continuing education and degreed programs that can develop and enhance the requisite skills necessary to heighten cyber resiliency across the nation and even the world. This solution offers a revenue stream to the academic institution at little to no cost or resource expenditure and produces more highly skilled graduates.

Ms. Linda Montgomery founded her business, Cyber World Institute, in 1985 with the early introduction of PCs. Over the past 32 years, her company has evolved and morphed to a leader in global cybersecurity workforce development. Today Cyber World Institute delivers training and education globally through business and academic partnerships. Authorized by four of the five global credentialing bodies ISC2, ECCouncil, ISACA, and CompTIA, CWI is changing the workforce development paradigm by delivering experiential based learning with cyber range labs. She currently serves as Co-Chair of the NICE – National Initiative for Cybersecurity Education, a DHS/NIST initiative, leading the Training and Certification Working Group.

Ms. Montgomery has a passion for veterans, as a wife, mother, and community leader involved in veteran's initiatives serving as Chair of the Veterans Community Commission (VCC). The VCC's mission is to provide a collaboration of services to veterans in the areas of Wellness, Education, Employment, and Relocation (attracting veterans to the state and communities).

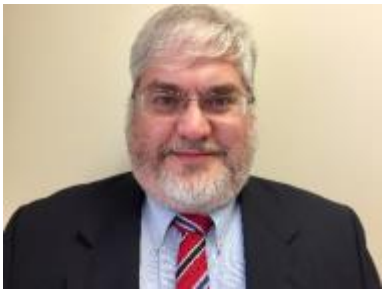
508 Compliance – Considerations for Training Programs

Craig Holcomb, NSA (Retired), Moderator
Bruce Bailey, U.S. Access Board
Mark Rew, DoD Computer/Electronic Accommodations Program's (CAP)

In 1998, Congress amended the Rehabilitation Act of 1973 to require Federal agencies to make their Information and Communication Technology (ICT) accessible to people with disabilities. Inaccessible technology interferes with an ability to obtain and use information quickly and easily. Section 508 was enacted to eliminate barriers in information technology, open new opportunities for people with disabilities, and encourage development of technologies that will help achieve these goals. The law applies to all Federal agencies when they develop, procure, maintain, or use Information and Communication Technology. Federal contractors producing products and services for Federal agencies must also must follow Section 508 requirements. Some state laws, such as Virginia, require state executive branch agencies and institutions of higher education to comply.

On January 9, 2017, the Access Board released a final rule that updates accessibility requirements for information and communication technology (ICT). This final rule is effective March 20, 2017. However, compliance with the section 508-based standards is not required until January 18, 2018.

While many Federal Agencies have Section 508 Coordinators who are responsible for organizing and supporting the implementation of Section 508 within their respective departments and agencies, this session allows you to learn of new requirements and ask questions improving accessibility for your workforce training initiatives.



Bruce Bailey has lead responsibility for the agency web site and with providing technical assistance on Section 508 as the policy relates to web sites and software. Bruce has been working for over twenty years in the field of assistive technology, and more than ten of those years in the Federal government. Bruce also is an invited expert with the W3C WAI Web Content Accessibility Guidelines Working Group and an ex officio member of the National Instructional Materials Accessibility Standards (NIMAS) Board.

Mark Rew serves as a Program Analyst for the Department of Defense (DoD) Computer/Electronic Accommodations Program (CAP), a centrally funded program which provides free assistive technology and training to wounded Service members and employees with disabilities at 69 partnering federal agencies. With over 32 years of federal service, CAP has benefitted greatly from Mr. Rew's contributions since he joined the program in 2003.

Mark began his federal career in 1984 as an IT Specialist for the National Weather Service. During his tenure with the National Weather Service, Mr. Rew received numerous recognitions, including in 2000 when he received a technology award for the accessibility of the website www.weather.gov.

Mark currently serves as CAP's Assessment Team Leader. In this role, he leads the team which is responsible for identifying appropriate assistive technology and services to allow individuals to perform their job responsibilities. Mr. Rew is CAP's blind, low vision and cognitive subject matter expert, and during his tenure as an Assessment Specialist, he has been the caseworker on over 17,000 individual accommodation requests. These have resulted in in the provision of more than 23,000 accommodations for civilian employees with disabilities and to wounded, ill and injured Service members. As part of these duties, Mark has conducted over 1,300 needs assessments to ensure individuals receive the most appropriate assistive technology based on their needs.

Mr. Rew is also active with the Section 508 Coordinator's Committee, working to ensure the accommodations CAP provides will operate in the customer's information technology environment. He is also active in managing CAP's IT infrastructure and development, by leading the team that develops, maintains and enhances the CAP database, website and other IT systems. In 2012, he received a disabled employee of the year award within the Department of Defense.

Mark has been a selected speaker on disability and employment issues at a variety of conferences, including: the Assistive Technology Industry Association (ATIA), the Center on Disabilities at California State University, Northridge (CSUN), and the American Counsel for the Blind Convention.

Mr. Rew earned a Master of Science in Computer Science from Bowie State University and a Bachelor of Science in Computer Science from University of Maryland – University College.

Mr. 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. Served as NSA's Section 508 Coordinator, responsible for ensuring NSA properly implemented the Section 508 Act law requiring Federal Agencies to provide equivalent access to Electronic and Information Technology (EIT) for people with disabilities. 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.

Cybersecurity: Decisions, Habits, and Hygiene

Servio Medina, Acting Policy Branch Chief, Cyber Security Division, Defense Health Agency

What do marketing, psychology, and good hygiene have to do with cybersecurity? Most incidents in the cyber domain can be traced back to human error. According to a recent study, mistakes are cited as the root cause of half of data breaches in healthcare. Understanding the choices people make and the habits they rely on will help us understand the relationship between human error and cyber incidents, and spark discussions on how we can affect sustainable changes.

Desired Learning Outcomes:

1. Demonstrate the inadequacy of today's cyber security training and awareness efforts.
2. Recognize how human behavior contributes to cyber incidents.
3. Illustrate ways to track and trend incidents that can trace back to bad choices and habits.
4. Explore innovative approaches to enhance cybersecurity awareness and understanding.

Servio Medina currently serves as the Defense Health Agency (DHA) Cyber Security Policy Branch Chief where his current work focus includes harmonization of policy objectives for Army, Navy and Air Force medical commands migrating to the DHA and the new Medical Community of Interest (Med COI). His tack is to communicate, clarify, and, only if really needed, create cybersecurity policy. Servio's tenure in the Military Health System began in 2003, which has focused primarily on cybersecurity and HIPAA Security. Prior to joining the DHA as a Federal employee, he worked as a cybersecurity policy consultant at Booz Allen Hamilton for 12 years. Earlier, Servio adjunct lectured mathematics at the University of Florida (at which he earned a Masters in Mathematics), and then taught the same at Stetson University in Deland Florida as a member of the faculty. In 2001 he was awarded a Hand Course Development Grant at Stetson University: "Introduction to Cryptology" with Dr. Hari Pulapaka, who continues to teach and improve the course today. Servio continues to innovate ways to make cybersecurity awareness contagious, and remains a recovering educator with 10 years teaching mathematics. Other interests include Cycling, Ultimate Frisbee, Japanese, and keeping up with his three kids and wife.

Improving Security and Privacy Awareness through the CMS Data Guardian Program

Karen Mandelbaum, Director, Security, Privacy Policy & Governance, Centers for Medicare & Medicaid Services and Micah Batchelder, CMS HHS

CMS understands that improving the cyber hygiene of the Agency requires a change in culture and a realignment of responsibilities within the organization. It is an Agency priority to enhance IT security strategies. Raising situational awareness to the risks and threats that persist in the digital world we operate in reduces the likelihood that an incident will occur but if/when an incident does occurs, we are prepared. CMS launched the Beneficiary Data Protection Initiative to ensure all members of our workforce understand the sensitivity of our data and the important role personal information plays in accomplishing our goals and mission. The Data Guardian program serves as a communication mechanism and the Data Guardians serve on the front lines of their respective Center/Office. They are responsible for disseminating the message that fortifies the culture and encourages staff to stop, think, and ask before taking a risk that could potentially compromises the IT systems or data of the organization.

The objectives of the Data Guardian Program include ensuring that:
• The workforce is aware of the current cybersecurity landscape that may affect the way we do business.
- Monthly Threat Briefs introduce Data Guardians to current cyber events and other relevant topics.

• A coordinated and consistent approach to the CMS security and privacy posture is applied across the enterprise.
- Monthly Policy and guidance updates provide Data Guardians with the most up-to-date information related to federal requirements.

This briefing will provide an overview of the Data Guardian Program at CMS and will showcase our successes using Phishing exercises and Tabletop exercises to train our workforce to recognize threats, avoid risks and respond with precision.

Karen Mandelbaum is an attorney with legal, policy and technical experience in healthcare and IT industry matters. Karen is currently working as the Director of the Division of Security Privacy Policy and Governance at the Centers for Medicare & Medicaid Services (CMS) to strengthen and integrate the information system security and privacy programs. Karen was integrally involved in defining and developing the security and privacy standards that apply to the Innovations and Health Insurance Marketplace programs under the Affordable Care Act. Prior to working at CMS, Karen was an attorney, practicing in Minnesota and advising on contracting, compliance, and regulatory affairs issues that uniquely affect healthcare organizations. Prior to practicing law, Karen worked as the Compliance Officer for a software developer providing cost and quality analyses to health insurers and health plans. Karen earned her law degree from William Mitchell College of Law and holds a Master's degree in Healthcare Administration from the University of Minnesota, Carlson School of Management.

Micah Batchelder is a Cybersecurity Professional with a background managing a Security Operations Center. Micah's experience includes, technical expertise in Forensic Analysis, Network Security, Malware Analysis, Vulnerability Management, and Incident Response. Micah has a Master of Science in High Technology Crime Forensics (Digital Forensics and Incident Response) from George Washington University, and a Bachelor of Science in Political Science from Rutgers University.

Cybersecurity Education and Awareness Training: A Societal Project

Professor Jim Chen, Ph.D., DoD National Defense University

Slides will not be posted.
Uncle Bob has retired from work for several years now. His computer has just been hit by a virus. Where can he get the help? Alice's six-year old kid was playing an online game on a smart device. Now that device acts weirdly. Where can they get the help? To help all of them to learn a lesson, where can they go?

Cybersecurity education and awareness training are urgent for society as a whole as people need to protect their families, businesses, organizations, and country in a hyper-connected world. This requires every citizen of the society, young or old, be engaged in cybersecurity education. At minimum, they have to know the consequence of not protecting the devices that they are using and some ways of protecting these devices. This presentation examines the current approaches in cybersecurity education and awareness training, analyze their issues such as the lack of support for senior citizens and youngsters as a society. It investigates the root cause of the issues. Then it explores new ways of conducting cybersecurity education and awareness training using varied venues and attractive methods.

Dr. Jim Chen is Professor of Cybersecurity in the College of Information and Cyberspace (CIC) at the DoD National Defense University (NDU). His expertise is in cybersecurity and national security, cyber strategy, cyber warfare, and cybersecurity education. He has published widely on these topics. He is a recognized cybersecurity expert.

The Importance of Gamification for Cybersecurity Team Training and Readiness

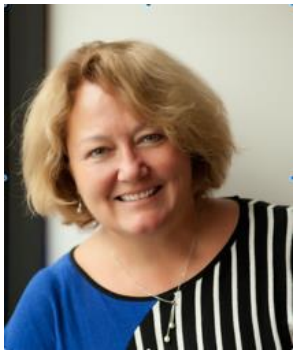
Laura Lee, Vice President of Cyber Training and Assessments, Circadence Corporation

Circadence has leveraged its history in multi-player game development, cybersecurity exercises and a deep understanding of machine learning to offer Project Ares - the only fully-immersive, Artificially Intelligent-powered, cybersecurity training platform in the market today. Project Ares provides cybersecurity teams the opportunity to practice skills to protect their networks and readily identify vulnerabilities and threats. Cybersecurity teams can hone tactics in realistic, mission-specific virtual environments with real-world tools, and network activity, available 24/7.

Typically, cybersecurity professionals are well-versed with their own tools; however, they still lack proficiency in the ability to defend their network as a team, potentially allowing threat actors to slip between the cracks. A team of talented basketball players can still lose the game if they aren't communicating and working well as a team! Communication regarding threat indicators of compromise is particularly challenging across the rapidly evolving multitude of tools used in Security Operations Centers. Cybersecurity teams need a mechanism to improve on their team dynamics to most effectively defend their network.

Not only does Project Ares provide relevant, effective gamified learning, it also introduces Artificial Intelligence (AI), machine-learning components as a computerized advisor, umpire and adversary. The AI components provide on-demand help and instant feedback to trainees, which results in freeing up the trainer's time to help other trainees or facilitate more focused orchestration tactics.

Laura Lee is the Vice President of Cyber Training and Assessments at Circadence Corporation. She brings an exceptional record of leadership in the field of cyber exercises and training, previously directing the research and development at Johns Hopkins University/Applied Physics Lab (JHU/APL), prior to joining Circadence. At Johns Hopkins, Laura developed the first ever Cyber Protection Team Crew Operations Manual for US Military Forces and National Guard Teams. In support of US CYBERCOMMAND, she led the assessment of cyber teams at large scale cyber exercises and developed team defense strategies for effective roles and techniques against Advance Persistent Threats. Laura's concept of a Special Forces-like A-Team for cyber defenders has proven invaluable to both our military and commercial clients.



At Circadence, Laura shares her cyber expertise with our Artificial intelligence advisors in order to build in-game avatars to help instruct players. She is leading our team of experienced game designers to create an immersive and engaging Cyber platform that embeds real-world cyber ranges in an Ender's Game-like environment. Laura applies her extensive knowledge of the National Institute of Standards and Technology (NIST) Cybersecurity Framework to create a detailed metrics and analysis capability that helps players understand the ground-truth of a cyber attack and their performance strengths/weaknesses.

Laura holds a Bachelor of Science in Aerospace Engineering from the University of Minnesota and a Masters of Science in Aerospace Engineering and Mechanics from the University of Notre Dame. She also has a Juris Doctorate from George Mason University School of Law. Laura is a Certified Information Systems Security Professional (CISSP) and holds certifications in gamification and game development.

NIST Walking Tour

Prize Drawings at the end of the Day in the Green Auditorium @ 4:45

Dinner Social at local restaurant TBD
Sign up at registration desk so we can provide a headcount.
Dinner is not included in the registration fee.

Wednesday, March 15, 2017

Green Auditorium	Morning Announcements: Clarence Williams, FISSEA Chairperson

Keynote: Achieving Critical Mass in Cybersecurity Education

Laurin Buchanan, CISSP, Principal Investigator, Secure Decisions

Slides will not be posted.

Researching decisions made by cyber defense analysts led to reflections on the current state of cybersecurity education: Cybersecurity decisions are being made, but are they the decisions that NEED to be made, or the simply decisions we have the data to make? Are we, as a community, teaching what needs to be taught for future success, or what we individually have the ability to teach? How might we achieve critical mass in cybersecurity education so that innovation has a sufficient rate of adoption to become self-sustaining and create further growth?

Laurin Buchanan spent two decades managing IT operations and information security in the corporate sector, most recently for a Fortune 1000 company. She now uses that operational background to lead R&D efforts for new and novel solutions to improve the cybersecurity decision making by humans in the loop, from automating decision support for network security policy management, to modeling and automatically mapping dependencies between missions, users, and cyber assets. Most recently she has worked to understand the decision processes of Computer Network Defense analysts and the use of visualizations to enhance those decisions, and to develop a novel, interactive approach for cybersecurity education and evaluation that addresses diverse age and expertise levels.

Cybersecurity Leadership: The Missing Link

Dr. Emma Garrison-Alexander, Vice Dean, Cybersecurity & Information Assurance, University of Maryland University College (UMUC)

The world of cyber continues to evolve and accelerate at an unprecedented pace. The proliferation of computers and mobile devices, and the need for businesses to operate in the digital domain, pushes the need for the right type of leadership. While technology is at the heart of the cybersecurity challenge, an informed and knowledgeable leader who understands the vulnerabilities and threats to an organization is **crucial** to ensuring the protection of data and assets.

Dr. Emma Garrison-Alexander serves as the Vice Dean of the Cybersecurity and Information Assurance Department in the graduate school at the University of Maryland University College (UMUC). Prior to this position, she was the Program Chair of the Cybersecurity Program and Assistant Collegiate Professor. She was also an adjunct faculty for the Cybersecurity Policy Program.

Previously, she served as the Assistant Administrator for Information Technology (IT) and Chief Information Officer (CIO) for the Transportation Security Administration (TSA) under the Department of Homeland Security (DHS). She led TSA's IT organization with an annual budget responsibility of $400 million. She provided all aspects of IT services for over 60,000 employees at 450 federalized airports and 23 international locations. She was responsible for all aspect of cybersecurity and information assurance, application development, infrastructure engineering, business management, financial planning and budget execution, and strategic planning. She was an integral part of the TSA Senior Leadership Team. She also played a key leadership role as a part of the Department of Homeland Security Chief Information Officer Council.

Prior to TSA, Dr. Garrison-Alexander served 25 years with the National Security Agency (NSA)/Department of Defense, starting as an Electronic Engineer and holding leadership positions in Technology and Systems, Signals Intelligence, Information Assurance, and Research & Development. She served as the Deputy Counterterrorism and as a Senior Operations Officer. She worked with all military services: Army, Navy, Air Force, Marines, and Special Forces. She was a part of the Defense Intelligence Senior Executive Service (SES).

She holds a Bachelor of Science in Electrical Engineering, a Masters of Science in Telecommunications Management and a Doctor of Management -Technology and Information Systems track.

Morning Break 10:10 – 10:40
Visit the Vendors and see security contest entries - Poster Hallway

Two tracks from 10:40 to 12:15

Cyberbullying/Cyber Harassment: The Facts, Methods and Reality

Dr. Karen Paullet, American Public University System

In order to fully understand cyberbullying it is critical that adults understand the consequences that can occur from inappropriate communication taking place in the digital world. As technology continues to change so do the methods used to bully and harass. Parents and educators must be aware of the inappropriate behaviors associated with the use of technology. One of the biggest challenges is anonymity. Often times it can be difficult to figure out who is actually sending the threats. It is imperative that parents, teachers and law enforcement work together to solve this growing problem. Topics to be discussed include cyberbullying, cyber harassment, sexting, predators, the dangers associated with social networking and the laws surrounding these issues.

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.

System Owners or System Renters

Tyler Wood, Information Assurance Branch Chief, Diplomatic Security, Department of State; Mike Petock, Function Manager and SME, Information Assurance Branch Department of State

Do the owners of the systems at your agency act like system owners... or like system renters? In this session we will discuss the thought process during the design and development of the Department of State Information Assurance for System Owners course. We will discuss the tasks and objectives, the course topics, and the activities and assessments included in the course. We will also answer questions on how to develop training to help your system owner act like one.

Tyler Wood is a Security Engineering Officer with the Department of State's Bureau of Diplomatic Security. Mr. Wood is a career member of the Foreign Service, currently serving as the chief of the Information Assurance Branch at the Diplomatic Security Training Center in Dunn Loring, VA. He leads a team of cybersecurity experts to teach role-based Information Assurance courses to the Department of State and other federal agencies.

Since joining the Department of State in 2005, Mr. Wood has had a variety of overseas assignments including Pretoria, South Africa; London, United Kingdom; Tbilisi, Georgia; as well as multiple assignments in Washington, DC. His areas of specialty include Information Assurance, technical security, technical counterintelligence and physical security.

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.

How to Create Animated Videos on a Shoestring Budget – and Why

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

Are you competing for your users' attention and need to get through to them? Do you want to take advantage of new technologies, but lack the resources? Join us to learn how you too can create animated videos that can solve many of your training, awareness, and marketing woes. We will take you step-by-step through the creation of our award-winning Security Byte videos, and give you the skills and knowledge you need to get started on your own videos right away. We will discuss several tools, workflows, and best practices that you can implement easily without sacrificing your annual budget.

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 Graduate Certificate in e-Learning from George Mason University, and her B.S. in neuroscience from Brigham Young University. Her previous positions include teaching assistant for the college of nursing study abroad program at BYU, and e-learning coordinator at the National Science Teachers Association. The author and artist behind the *Security Bytes*, Stephanie enjoys bringing entertaining and educational information security materials and courses to the NIH audience. In her spare time, she can be found playing the piano, working on a sewing project, or preparing her next lesson for the children's Sunday school class she teaches. Stephanie and her husband are happily expecting their first child, due in May.

Hidden Universes of Cybersecurity Awareness

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

Looking for an endless supply of cybersecurity training resources? Trying to find the best quality resources? During this briefing, I could just give you an amazing, impressive, huge, massive list of cybersecurity links. However, as fellow cybersecurity educators, I know you would agree with the proverb:

"Give a person a Phish, and you feed them for a day,
Teach a person how to Phish, and you feed them for a lifetime."

I will teach you how to quickly find the best resources for any topic using several very clever and efficient search techniques. (And yes, there may also be an amazing, impressive, huge, massive list of cybersecurity links).

Russ Haynal Since 1994, Russ has provided customized 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, international partners and numerous companies. Russ helps organizations succeed by ensuring their Internet usage is efficient, thorough, and secure. He teaches analysts and researchers how to quickly find the most useful information located anywhere in the online world, while always promoting Internet Tradecraft methods and cyber security concepts to minimize inadvertent leaking of research topics. His course "Hidden Universes of Information on the Internet" is an elective for analysts pursuing the ICAAP certification (Intelligence Community Advanced Analyst Program). Russ has also presented at many events such as nine annual National OPSEC Conferences. He is a founding officer of the Washington DC Chapter of the Internet Society.

Establishing a Strong Cybersecurity Front by Utilizing Cybersecurity Governance

Kimberly Blake, Policy and Security Awareness Lead, Indian Health Service (IHS)

As more cybersecurity threats emerge and spread, agencies and organizations are establishing positive change to face security challenges. Consequences of weak security are realized by our leadership and adapting a cybersecurity framework through governance is essential. It is extremely important to ensure that plans are in place, technical controls are implemented, audits and assessments are well documented, and that we continue to drive awareness to improve security behavior. Strong policy enhances agency preparedness, training objectives, cybersecurity project initiatives, and ongoing undisruptive patient care by providing an established cybersecurity framework. The Indian Health Service has implemented a project plan to address all NIST 800-53 security control families in policy. We will share our workflows, tracking, and working group strategies that organizations may be able to utilize. Policy processes from agency to agency can be different however, the Indian Health Service Cybersecurity Program strives for continuous improvements for internal collaboration as well as management of policies, a collective need among organizations. We will also share how policy ties into training, leadership buy-in, and improved implementation of security due diligence.

Kimberly Blake is the Policy and Security Awareness Lead for the Cybersecurity Program at Indian Health Service. Mrs. Blake's experience includes developing and implementing cybersecurity policy, awareness programs, training, design, and marketing materials. She has dedicated over 5 years of service in the health sector and seven years in the private sector.

At the Food and Drug Administration (FDA) she directed significant improvements in user behavior through annual cybersecurity training, awareness campaigns, policy, and cutting edge design. Mrs. Blake continues her passion and commitment at the Indian Health Service. She collaborates across the government, and enjoys utilizing her skill set to help strengthen agencies security posture. Mrs. Blake along with her team was awarded the CSO Magazine – CSO50 Award in 2016, FDA Office of Operations award for Excellence in Communication, FISSEA peer choice award for poster and website in 2015, FISSEA motivational item and peer choice award for website and newsletter in 2014, FISSEA website, newsletter, and peer choice award for website and newsletter in 2013, and FISSEA motivational item and newsletter award in 2012.

Mrs. Blake earned a Master of Science (M.S.) in Cybersecurity from University Maryland University College. She holds a Graduate Certificate in Foundations of Cybersecurity, Graduate Certificate in Cybersecurity Technology and CompTIA Security+ Certification.

How Table Top Exercises Engage and Train Technical and Non-Technical Staff in Better Cyber Human Behavior and Operations

Geoff Hancock, Advanced Cybersecurity Group

Effective responses to cybersecurity incidents rely in large part upon three key elements: trained personnel, planning and practice. Cybersecurity Tabletop exercises help organizations train personal at all levels and help teams analyze potential situations in an informal environment. They are also designed to foster constructive discussions among participants as they examine existing operational plans and determine where they can make improvements.

Responding to cybersecurity issues requires capable personnel with the appropriate authority to act, requisite expertise and adequate training. An organization also needs a written plan customized to meet its business, industry and regulatory environment, among other things.

Using the tabletop exercise as a way to train employees on human cyber hygiene as well as identifying operational or technical weakness, puts the reality and responsibility of securing an organization in everyone's hands and eliminates the idea that it is just a technical issue.

These exercise bring together people from across the organization, to clarify common expected risks in the organization and identify the areas of higher risk. They are excellent for helping staff understand their role in securing the organizing and how people work together to protect information.

Tabletop exercise can give an organization confidence that in the event of certain crises or situations, people are trained to perform well and understand the daily responsibilities of security. And, when difficulties and issues arise, the findings from an exercise can form a blueprint of clear action items that the organization can prioritize and implement for greater peace of mind.

Geoff Hancock is currently principal at the Advanced Cybersecurity Group. Where he supports government, commercial and start-up companies in various cybersecurity programs. He has been in Cybersecurity for 26 years. With experience across the US government and the top 50 commercial companies. He has held positions such as CISO, CTO, VP and General Manager across the intersection of business and Cybersecurity. He has conducted table top exercises for commercial and government organizations for more than 10 years.

He is an adjunct professor at George Washington University and co-founder of the Cyber Intelligence Institute at the Institute for World Politics. He is also the Chief of Cybersecurity Solutions for KnowCyber a Training and Education company. Geoff has spoken at many cybersecurity conferences on cyber operations, insider threat, active defense cyber training and education and other specialties. Geoff also work with the White House on EC 13636 and the follow on NIST Critical Infrastructure Framework. He is a team member on two NICE Workforce committee's focused on developing the cyber workforce.

Lunch – 12:20 – 1:10 pm

- There are no lunch tickets this year.
- 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.

Visit the Vendors and see all security contest entries - Poster Hallway

Pecha Kucha

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: Sandy Toner, Half an Octopus**

- **Unleashing the Power of Stories for Cybersecurity Education**
  Laurin Buchanan, CISSP, Principal Investigator, Secure Decisions

Educators need tools to help impart memorable and meaningful lessons, however, explaining cause and effect of cyber events can be difficult: they don't always occur in a context that is easily or immediately visible. Stories are powerful teaching tools: they build on prior experience through analogy and metaphor, and can be used with any age or expertise group. Branching, graphic "choose your own adventure" stories take it further by letting readers make choices on behalf of a character, causing the story to follow a variety of branches with different outcomes. These stories represent a novel genre for teaching cybersecurity because these stories give the learner an opportunity to make decisions and, more importantly, explore the consequences of those decisions in a safe environment.

This lighting talk discusses Comic-BEE, a web-based solution that enables cybersecurity educators to rapidly develop these branching, graphic stories aligned with desired learning objectives, without requiring a programmer or graphic artist. The stories can be used for education as well as assessment, and the technology is currently free for government use. Comic-BEE is based on research sponsored by the Department of Homeland Security (DHS) Science and Technology Directorate, Cyber Security Division (DHS S&T/CSD), and is currently being evaluated under a grant from NSF.

- **(Effective anti-phishing strategies/exercises) "Dan got phished: Here's how he's fighting back and you can too."**
  Hoala Greevy, Paubox, Inc.

- **30 Years of Change**
  Description: A quick trip from then to now.
  Gretchen Morris, DB Consulting/NASA

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.

- **2274.US: The Security of PII**
  Steven Bledsoe, Founder, 2274 Inc.

How to integrate the emotional attachment of money to teach everyone about the importance of Cybersecurity. We will focus on the blue / green intersection “Security of PII”. The overview will cover the information released on how privacy and information security intersect.

Steven Bledsoe | Apple Teacher with Swift Playgrounds recognition.
CSUN13 B.A. Cinema and Television Arts
Electronic Media Management
2274 Inc. Founder
Webmaster | Privacy Engineering
X USC Marshall MMLIS cohort XI

Two tracks from 1:45 – 3:30

Cybersecurity Learning Assets for the Federal Workforce: What Works?

Susan Hansche, Training Manager, Department of Homeland Security and Jim Wiggins, DHS Contractor

I want training, I need training… well, not that kind of training! I want training in a classroom with an instructor, I want online, on-demand training, I like youtube video’s, I want to read a paper, I want a hands-on lab, I want this, I want that, actually, I don’t need training, just tell me what I need to know! As training designers, we stand by the theory that the training medium is decided by matching training content to the best delivery mode. It’s a good theory, but what if the stakeholders have a different idea of how training should be delivered. In this session, we want to hear your successful and not so successful training delivery mediums – we will share some of what we have been doing, but we are seeking a dialogue with our FISSEA colleagues to discuss what works!

Ms. Susan Hansche, CISSP-ISSEP, has been a FISSEA supporter for many years and is honored to present at the 30th Annual FISSEA Workshop. She is the Training Section Chief in the Federal Network Resilience division 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. 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.

In 2012, Ms. Hansche was honored to receive FISSEA recognition as the Educator of the Year, which recognizes an individual who has made significant contributions in education and training programs for information systems security.

Jim Wiggins has over 19 years direct experience in the design, operation, management, and auditing of information technology systems, with the past 15 years focused on information systems security. He has an extensive background in technical education and specializes in security certification courses targeted at federal and government contracting clients.

Additionally, Jim is the founder and executive director of the Federal IT Security Institute (FITSI). FITSI is a 501c6, non-profit organization that provides a role-based IT security certification program targeted at the federal workforce.

Jim is also the executive director of the FITSI Foundation. The FITSI Foundation is 501c3 public charity that runs the Wounded Warrior Cyber Combat Academy (W2CCA).

Currently as a contractor, Jim provides education and training support for the Federal Network Resilience Division at DHS and its Continuous Diagnostics and Mitigation program.

In 2011, the Federal Information Systems Security Educators' Association (FISSEA) named him "Educator of the Year" for the impact he continues to make in the federal workforce.

Jim holds the following IA/IT security certifications: CISSP, ISSEP, CISM, CISA, SCNA, SCNP, CAP, IAM, IEM, SSCP, CEH, ECSA, CHFI, LPT, TICSA, CIWSA, Security+, and MCSE: Security and FITSP-M.

Gone Phishing, an Anti-Phishing Program Journey

Ava Logan-Woods, Information Security Specialist, CACI International Inc. and Eshante Lovett, CACI International Inc.

It is often stated that humans are the greatest risk to information security. CACI provides information solutions and services in support of national security missions and government transformation for Intelligence, Defense, and Federal Civilian Customers. Understanding the cybersecurity risks associated with employees in this industry factored into the decision for CACI to incorporate anti-phishing training as part of its Security Awareness Program in 2010. This session will review CACI's anti-phishing journey beginning with exploring the need for an anti-phishing program through lessons learned and moving the program forward. We'll focus on proving the value of an anti-phishing program, the cultural changes needed to develop a successful program, program outcomes and reporting. The goal is to provide attendees with the steps they need to develop an anti-phishing program along with an idea of what challenges they may face when implementing and growing their program.

Ava Logan-Woods is an Information Security Specialist supporting the Information Security Awareness Program at CACI International Inc. She has a B.S. in Cybersecurity from the University of Maryland University College. Her previous positions include data governance and metadata management training and customer support roles for a large credit union. Ava is an Advanced Communicator and Advanced Leader with Toastmasters International. She enjoys being creative in delivering information security awareness materials and training to CACI employees. Ava lives with her husband and three dogs in Virginia.

The Role of Positive User Incentives in Reducing Insider Cyber Threats

Albert (Al) Lewis, Principal Examiner, Federal Housing Finance Agency (FHFA)

Insider threats are currently responsible for 60 percent of attacks facing organizations, according to IBM. Recent research by Carnegie Mellon University Software Engineering Institute (SEI) indicates that by focusing on improving three areas of employee engagement – feelings of connectedness at work, perceived organizational support, and job engagement – organizations might positively impact the frequency of cybersecurity theft and sabotage. Come and join this discussion of possible positive incentives for reducing insider threat in your organization. We will also discuss the Carnegie Mellon SEI Insider Threat Program Evaluation (ITPE) model and how it can be used in your organization to assess your ability to identify and thwart insider threats.

Al Lewis has three decades of experience in systems integration, network security operations, and information risk management. For the past 15 years, he has led information security teams for the DoD, Energy, and the U.S. Supreme Court. He also served as cybersecurity policy and compliance lead for the MITRE Corporation. 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 and Telecommunication Systems Management from Johns Hopkins University, and is a Certified Information Security Manager (CISM) and a Certified Information Systems Security Professional (CISSP).

How the Internal Revenue Service (IRS) Created an Agency-Wide Professional Development Certification Program with No Money

James R. Lindley, IRS (Retired)

Faced with the agency-wide loss of substantial amounts of funding for travel and training, professionally certified IRS employees in the Cybersecurity division created a set of professional certification courses using only the skills of federal employees and already existing classrooms and online communications to extend training to several hundred IRS employees annually. All materials were either created by IRS employees or used books and other online materials available to all IRS employees, specifically Skillsoft[tm] courses, Books24x7[tm], and the IRS own Electronic Learning Management (ELM) courses. Many of these same online learning services and communication channels already are available to federal employees in other agencies. The classes were conducted without training or travel costs beyond the time spent by the instructors and students.

James R. Lindley is the former Chief Source Code Security Code Analyst for the Internal Revenue Service (IRS) Cybersecurity Penetration Testing and Code Analysis (PTCA) group. He has also been an IRS Senior Security Architect, Security Engineer, and Computer Engineer.

Prior to joining the IRS, he worked for the former Internet Security Systems Inc. as a product trainer, X-Force member, and Director of Training for Managed Security Services Security Operations Centers and for the former GuardedNet Inc as Director of Internal and External Training.

He retired as a Chief Warrant Officer (CW4) from the US Army with experience in Automated Data Processing, Signal operations, and various military intelligence areas. He was an instructor in several US Army technical and intelligence schools.

He has an AS in ADP from MPCC in Monterey CA, a BS in Liberal Studies from Regents College of New York, an MS/CS from SPSU of Marietta GA, and diplomas in Russian and Czech/Slovak from DLIFLC and in Broadcast Electronics from CIE.

At various colleges, he has been an instructor in speech arts, political science, audio-visual arts, and computer science and security. He is certified as a CISSP, ISSAP, ISSEP, ISSMP, CSSLP, PMP, SSE-CMM Appraiser, CHS-III, ICCP-C, CNSS 4013, A+, Network+, and Security+. He formerly held an MCSE, MCT, CNE, and FCC First Class Radiotelephony certificate.

Cyber Awareness Lights are On, but Nobody's Home

Sandy Toner, Half an Octopus

Traditionally, the focus on Information Assurance and Cyber Awareness programs in the workplace tend to be limited to the office and professional use of mobile devices. While this is a logical scope for training, extending awareness programs to include the home front has many benefits for the employee and the organization. By translating awareness activities to the home area network, employees gain a better understanding of risks and how their actions can reduce vulnerabilities. It is well documented in educational research that the absolute best way to increase your understanding and retention of a subject is to teach it to someone else or apply it to a different context. Given that the Internet of Things (IoT) has connected and extended the reach of employee activity, moving awareness training beyond the office only makes sense. In this presentation I will discuss how you can augment your cybersecurity training program with resources and information that enable employees to improve the cybersecurity awareness of their household. I will include examples of activities that can translate to an individual, a family, and roommates working to secure their myriad of networked home devices.

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.

The Exploitation of Minors to Gain Confidential Information

Tonya Mead, Certified Fraud Examiner (CFE), Private Investigator (PI), Shared Knowledge, LLC

The primary purpose of this presentation is to share information on the need to develop awareness, training and education programs to alert federal employees on the potential for criminals to use deceptive tactics to trick their children into divulging information digitally thereby gaining backdoor access to personal identifiable information and federal systems. A few scenarios will be shared illustrating the threat. Secondarily, we will briefly explore the types of confidential student data routinely submitted (as required) to federal agencies by schools and universities. The identification of pressures that increase the risk of exploitation of minors such as the lack of security preparedness and limits to technological resources will be discussed. Reports of the unintentional disclosure of millions of student records leading to aggravated identity theft abound. Finally, if time permits, the session will close by discussing the (1) ways in which agencies might broaden training to consider the extended family members of the federal workforce, (2) stress the importance of the (i) protection of the personal information of minors, and (ii) the need to increase the cyber awareness, training and education of the multi-level submitters of data-based reports to the federal government.

Tonya Mead, MBA, MA is a Certified Fraud Examiner, Compliance Agent, Private Investigator, Certified Regular School Administrator, and Certified School-based Psychologist. She has utilized data, information systems and business process re-engineering to solve complex problems. She solved the Washington, DC public school crisis surrounding the 2011-2013 educator cheating scandal that received national media attention from major news outlets such as USA Today, the Atlantic, Esquire, Washington Post, and NPR impacting 80,000 students, 11,000 educators and 54 District school superintendents. For her efforts, she received the 2014 Cafritz Award for Excellence in Government Service and Public Leadership. She is the author of Fraud in Education: Beyond the Wrong Answer which explores insider and outsider fraud, data and computer-assisted crimes in education. She is the president of Shared Knowledge LLC http://ishareknowledge.com a private security and investigations agency and author of Fraud in Education: Beyond the Wrong Answer which explores fraud, data and computer-assisted crimes in education and updates her blog http://edfraud.net regularly.

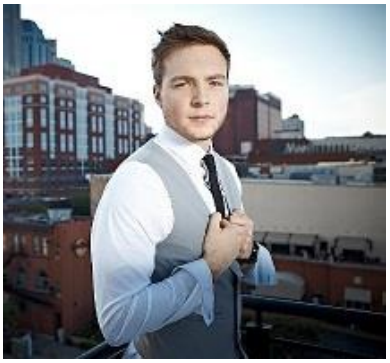
Back to one session in Green Auditorium

"Rock the Boat: Transforming Security Culture through Innovation"

Graham J. Westbrook, Cybersecurity Analyst, Geisinger Health System and W. Scott Lenker, Sr. Cybersecurity Analyst, Geisinger Health System

Traditional security education programs tend to live within the boundary of an organization's culture, emphasizing compliance and resisting radical ideas. At Geisinger Health System (GHS), we have opted to challenge this norm. Our goal is to transform the culture rather than work comfortably within the box. We contend that in order to create a security culture, an information security department must be innovative, creative and – to a degree – non-conformist. It is not enough to plug 'n play the latest security training solution. Security teams must employ unorthodox training methods and 'rock the cultural boat' because, in the moments following the tilt, those aboard become simultaneously aware of their surroundings and uncomfortable enough to act quickly – two characteristics that help right the ship and chart new course. In security terms, this translates to a workforce capable of making sound technical decisions.

In this session we will present lessons learned from our own journey and hope to assist others who want to rock the boat and begin transforming their own security culture.



Graham J. Westbrook (Sec+, C|EH) is a cybersecurity analyst with Geisinger Health System's Information Security Office. As an intelligence analyst by training and cybersecurity analyst by trade, Graham merges the disciplines to run the Threat Intelligence and User Awareness programs at Geisinger. Past experience includes time with a Defense Contractor, Foreign Policy firm and a Nashville-based tech company.
(photo on left)

W. Scott Lenker (CISSP, C|EH, CPT) entered into the Information Technology field over 25 years ago. He held various positions in the Insurance, Financial, and Healthcare verticals, including Network Architect, Senior Systems Engineer, and Senior Information Security Engineer. Currently he is employed by Geisinger Health Systems as a Senior Information Security Analyst responsible for Geisinger's southern information security operations.

Cybersecurity – The Human Factor

Dave Witkowski, Managing Director, Deloitte Consulting; Lisa Holman, Acting Deputy CISO, U.S. Postal Service; and Pilar Jarrin, Manager, Deloitte Consulting

Human factors play a vital role in the information security of an organization. Security begins with people - their behaviors, their motivations, and an organization's ability to manage its cyber workforce. In this session, presenters will discuss (1) how leaders can analyze and transform the human factors of an organization to build a culture of shared ownership for cyber risks, (2) how to set up partnerships with leadership across organizations and ensure that leadership engage and support cybersecurity programs, and (3) share some success stories where organizations have done so.

The session will begin with the overview of various human factors that impact the information security of the organization. The speakers will then discuss the challenges that organizations face in becoming strategic security organizations and the ways to overcome these challenges, including leadership partnership and engagement.

The second half of the session will focus on the strategies how the human factors can be modified to create an organizational culture that has positive impact on the security of the organization. The speakers will explain the role of Culture, Organizational and Talent Strategies, Employee Engagement, Change Management, and Learning and Leadership Solutions in enabling an organization to become a strategic security organization.

Dave Witkowski leads Deloitte's Cyber Organization and Talent practice, advising federal government IT executives on cybersecurity workforce strategy. Focusing on key issues in the cyber workforce such as the gap between talent demand and supply and the evolving nature of cyber threats, the team's work includes leadership assessment, workforce planning, training and awareness, competency modeling, hiring sourcing strategies, and organizational change management. Dave has an undergraduate degree and an MBA from Cornell University and a Master's in Microbiology from the University of Virginia. He is a certified Senior Professional in Human Resources (SPHR) and Project Management Professional (PMP).

Lisa Holman is the Acting Deputy Chief Information Security Officer (CISO) at the U.S. Postal Service. Holman brings more than thirty years of Federal experience and cybersecurity expertise to the Corporate Information Security Office (CISO) and leads a number of its programmatic efforts, including risk management, physical security, emergency preparedness, awareness and training, and workforce development. Prior to this role, Holman was an Assistant Inspector at the U.S. Postal Inspection Service (USPIS), where she managed its IT applications and infrastructure and led efforts against internet crimes and child exploitation. Her efforts earned her a reputation as one of the best law enforcement professionals defending children across the nation. Her commitment to protecting customers, employees, and partners brings tremendous value to the Postal Service and the cybersecurity community at large.

Pilar Jarrin is a Manager within the Federal Human Capital practice of Deloitte Consulting. Ms. Jarrin specializes in managing change in complex operational environments and currently leads teams at United States Postal Service (USPS) to drive stakeholder and leadership engagement efforts that enable cyber compliance, including Sarbanes Oxley (SOX), Payment Card Industry, and OIG audit compliance within the CIO environment. Ms. Jarrin holds an undergraduate degree from Johns Hopkins University and a Master's in Public Policy from Georgetown University.

Conference Close – Clarence Williams

Stay to the end for prize drawings

NIST Launches Beta Site for the Computer Security Resource Center (CSRC)
2/23/2017

The NIST CSRC Redesign Team have been developing a new version of CSRC, and today you can access the beta release at https://beta.csrc.nist.gov. It will be available alongside http://csrc.nist.gov for several months as we continue to fix issues, implement enhanced functionality, and migrate existing content. (Most—but not all—of our current content has been migrated.)

A completely overhauled **Publications** interface includes significantly more publication details, historical documents, and external publications. Other primary CSRC content—**Projects**, **News**, and **Events**—are redesigned to better connect related content and provide a more consistent layout. We'll continue to refine a new **Topics** taxonomy that tags content site-wide. And soon we'll be adding an interactive, regularly-updated **Glossary** that is based on NIST's *Glossary of Key Information Security Terms*. And another big change you'll notice is a **responsive design** that should provide a better experience to mobile device users.

On the beta site, the page footer includes an email link to **submit your feedback**. We appreciate your input and will take it into consideration as we move forward.

Expect more changes in the months ahead! Eventually, the beta site will go "live" and replace what's at **csrc.nist.gov.** At that time, links to existing content will automatically be redirected to their new locations.

FISSEA holds an annual conference every March. Plan ahead for 2018.

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.

Clarence Williams, NIST, is Chairperson of the FISSEA Working Group as well as Government Lead for NICE. The Working Group members are from various agencies and organizations and volunteer their time. Former FISSEA Chairperson, Patricia Toth, changed divisions within NIST and is now with the Manufacturing Extension Partnership (MEP).

Peggy Himes has worked with FISSEA Executive Boards and Working Groups since 1998 and has been with NIST since 1991. This will be my last FISSEA Conference as I retire in June 2017. I have enjoyed all my years working at NIST on the FISSEA, FORUM and FISMA projects. FISSEA conferences are more like family reunions where bonds of friendship are formed and continue to grow. *Thank you all.*

FISSEA Working Group

Scott Anderson, Veterans Affairs (VA)	Servio Medina, Defense Health Agency
Daniel Benjamin, American Public University	Gretchen Morris, DB Consulting/NASA
Terry Brox	Louis Numkin, FISSEA Life Member (retired IRS)
Art Chantker, Potomac Forum	Loyce Pailen, UMUC
Brenda Ellis, NASA	Edna Reid, JMU
Susan Farrand, Dept of Energy	Mike Riley, EdgeSource/State
Edwin Games, NIST	Kimberly Sanders, Amtrack
Angela Guinn, VA	Cheryl Seaman, National Institutes of Health
Susan Hansche, DHS	Sandy Toner, Half an Octopus
Peggy Himes, NIST	Jim Wiggins, Federal IT Security Institute
Craig Holcomb, NSA, retired	Carl Willis-Ford, CSRA
John Ippolito, Consultant	Clarence Williams, NIST, FISSEA Chairperson
Lance Kelson, Dept of the Interior	Mark Wilson, FISSEA Life Member (retired NIST)
Al Lewis, Federal Housing Finance Agency	

Thank you…..

It takes a team to make it work.

- **Speakers for donating their time, energy, and knowledge**.

- **FISSEA Working Group** members for their input on the program and assisting with on-site details. They truly are "working" members and can be counted on. Working group members are listed in the text box.
  - Gretchen Morris for coordinating the FISSEA Security Contest that continues to grow each year. She accepts entries, enlists impartial judges, and prepares all entries to share at the conference.
  - Many volunteered to MC and present.

- **American Public University System** for donating backpacks for all attendees – Daniel Benjamin and Brent Inscoe.

- **Potomac Forum**, Art Chantker, for contributing the FISSEA Educator of the Year plaque.

- **Federal Business Council** team for registration and donating frames for the Security Contest.

- Prize drawing contributors: *(they sure make the conference more fun)*
  - **Carl Willis-Ford**, Federal Health CTO, CSRA - (2x) Amazon Echo Dot 2nd Generation and (1x) Amazon Kindle Paper White

- NIST Applied Cybersecurity Division and Computer Security Division support:
  - Kevin Stine, NIST Division Chief, Applied Cybersecurity Division
  - Clarence Williams, NIST/NICE, FISSEA Conference Director
  - Peggy Himes, NIST, FISSEA Conference Administrator
  - Edwin Games, NIST, support and slide show of past brochures
  - Patrick O'Reilly and Nikki Keller for website maintenance

- NIST Public Affairs Office
  - Mary Lou Norris, NIST Conference Office Director
  - Crissy Robinson, designed the 30th FISSEA Anniversary Logo, our program cover and handled social media.
  - Karen Startsman, registration and logistics
  - NIST AV Technicians

- Conference presentations, receiving permission, will be posted after the conference to the FISSEA Website: http://csrc.nist.gov/fissea (see the earlier explanation about the redesign of CRSC)

- To be added or removed to the fisseaupdates@nist.gov mail list, email fisseamembership@nist.gov – conference attendees will be automatically subscribed.