Program Updates

June 19, 2017

Presentations, receiving permission, the Educator of the Year awardee nomination letter, and the Security Contest entries will be posted to the FISSEA website after June 19th. FISSEA Website http://csrc.nist.gov/fissea The FISSEA website will be undergoing a change in the next few months. The link to the FISSEA page on the beta site is: https://beta.csrc.nist.gov/Projects/FISSEA

The already printed March 14-15, 2017 Programs are being used since they include speaker bios and abstracts for those presenting for the one-day June 19th Meeting. Photos/bios appear in order of how they were on the March agenda. We apologize for any inconvenience but wanted to be cost effective and save paper by using the existing material.

Crissy Robinson of the NIST Conference Program will email an evaluation survey after the conference. Participant feedback is important to the conference committee, please share your thoughts by completing this survey. FISSEA conferences are for the community and we are seeking your input so that the conference theme, topics, speakers can address the issues you are facing today.

Prize drawings will be held at 4:30pm, you must be present to win, and are strictly optional for FISSEA participants. We would like to thank FISSEA Working Group members, Carl Willis-Ford, Federal Health CTO, CSRA for donating two Amazon Echo Dot 2nd Generation and an Amazon Kindle Paper White and Art Chantker for donating a Potomac Forum Training Workshop Registration (Value $6795 to $1395), as well as SANS for donating a Fire Tablet.

Planning a conference takes teamwork and we thank:

- Speakers for donating their time and expertise.
- NIST Applied Cybersecurity Division (Kevin Stine, Division Chief) for hosting the June meeting at no cost to attendees.
- American Public University (Daniel Benjamin and Brent Inscoe) for donating backpacks for all attendees.
- Potomac Forum (Art Chantker) for contributing the Educator of the Year plaque.
- Federal Business Council for donating frames for the security contest certificate winners.
- FISSEA Working Group Members for their input on the Program and/or volunteering to present or MC. Particularly, Clarence Williams, FISSEA Working Group Chairperson and Gretchen Morris, Security Contest Coordinator.
- NIST Conference Program Team (Mary Lou Norris, Crissy Robinson, Karen Startsman) for their logistical/registration conference support and the NIST AV Technicians (Akeem Henry, Joe Hynes and Hoyt Cox).

Changes to the March Program

NIST Welcome

Charles Romine, Director of the Information Technology Laboratory (ITL), NIST

Charles (Chuck) Romine is Director of the Information Technology Laboratory (ITL). ITL is one of six research Laboratories within the NIST with an annual budget of $120 million, nearly 400 employees, and about 200 guest researchers from industry, universities, and foreign laboratories. Dr. Romine oversees a research program that cultivates trust in information technology and metrology by developing and disseminating standards, measurements, and testing for interoperability, security, usability, and reliability of information systems. ITL develops and disseminates cybersecurity standards and guidelines for Federal agencies and U.S. industry. ITL supports these and measurement science at NIST through fundamental and applied research in computer science, mathematics, and statistics.

508 Compliance – Considerations for Training Programs

Bruce Bailey, U.S. Access Board
Helen Chamberlain, Program Director, General Services Administration (GSA)
Mark Rew, DoD Computer/Electronic Accommodations Program's (CAP)
Craig Holcomb, NSA (Retired), Moderator

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, Mark Rew, and Craig Holcomb's bios and photos are in the March Program.

Helen Chamberlain is a Program Director for the General Services Administration's (GSA) Office of Governmentwide Policy (OGP), Information Resources Management Division. She is the central point of contact for the Federal Government Section 508 training and outreach program providing technical assistance with the implementation of the Section 508 Standard within the Federal Government.

Before assuming her current position, Helen served as an Information Technology Liaison and IT Security Officer for the Office of Personnel Management, Chief Information Officer's Office (OPM/CIO). She also serves as a member of the Federal CIO Council Accessibility Community of Practice and co-chairs the Outreach Sub Committee.

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

Hoala Greevy, Paubox, Inc.

While fishing may be a relaxing sport, phishing is only sport for cybercriminals looking to exploit human vulnerabilities to steal or lockdown data, inject malware, take over systems and other malicious activity. This presentation will cover common phishing attacks that are being employed and what you can do to prevent them. This will include technical tactics such as leveraging the latest in technology to secure your network.

Hoala Greevy is the Founder CEO of Paubox and has 18 years' experience in the email industry, and is the architect of the Paubox platform. He graduated from Portland State University with a BS in Geography and a BS in Social Sciences. He likes to go kayak fishing when possible and has caught two blue marlins from his kayak. They were 150 lbs. and 168 lbs.

Cybersecurity – The Human Factor

Dave Witkowski, Managing Director, Deloitte Consulting;
Sarah Benczik, Senior Manager, Deloitte Consulting;
Pilar Jarrin, Manager, Deloitte Consulting and
Emile Walker, Manager Cybersecurity Awareness & Training, U.S. Postal Service

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 and Pilar Jarrin's bios and photos are in the March Program.

Sarah Benczik is a Senior Manager at Deloitte Consulting LLP. She advises government leaders on people-focused strategy to improve mission and business results. Her recent work has focused on cybersecurity workforce planning and management, integrating talent management processes with employee engagement to improve employee experience, and designing organization and governance structures for cyber organizations. She is an active contributor to Deloitte's thought leadership on cyber security workforce challenges and federal organization design and regularly facilitates strategy and human capital innovation working sessions. Sarah has a Master of Public Administration from Maxwell School of Citizenship and Public Affairs along with a Certificate of Advanced Study in Security Studies, a Juris Doctor from the Syracuse University College of Law, and is a certified Project Management Professional (PMP).

Emile Walker is the Manager, Cybersecurity Awareness & Training at the U.S. Postal Service. Walker has over 41 years of Information Security (INFOSEC) experience with the last 22 years of combined military, federal and corporate cybersecurity-specific expertise and experience. He currently leads a team of some 14 federal and contractor personnel who execute the USPS Initiative/Program responsible for ensuring Postal personnel awareness and training in the cybersecurity space. Prior to this Walker has had a broad range of cybersecurity experience including Information Systems Security Officer (ISSO), DoD CERT Incident Handler/Analyst, Unix/Linux Systems Administrator, Vulnerability Assessment Analyst, Site Security Reviewer, Websense Administrator and other related cybersecurity responsibilities. Walker is currently involved with the USPS Insider Threat (IT) Training Initiative and is certified as an IT Vulnerability Assessor (ITVA) and IT Program Manager (ITPM). Walker holds an Associate Degree from the Community College of the Air Force.