Federal Computer Security Managers' Forum

NIST Green Auditorium

Program

Tuesday, August 16, 2016

9:00 am – 9:10 am	**Welcome:** Patricia Toth, National Institute of Standards and Technology (NIST), FCSM Chairperson

Pat Toth is a Supervisory Computer Scientist in the Applied Cybersecurity Division at NIST. Her current project areas include information security, cybersecurity awareness, training and education. Pat is the lead for the Small Business Outreach, Chair of the FISSEA Technical Working Group, Chair of the Federal Computer Security Program Managers' Forum and co-author of SP 800-16 rev 1.

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

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

9:10 am – 10:10 am	**How to Best Protect Against Future Cyber Incidents:** Trevor H. Rudolph, Chief, Cyber & National Security Unit, Office of Management and Budget (OMB)

Trevor H. Rudolph is the chief of OMB's Cyber and National Security Unit, OMB's first ever dedicated team tasked with strengthening Federal cybersecurity through data-driven oversight and strategic policy implementation. In this role, Trevor is responsible for advising the Federal Chief Information Officer and White House leadership on Federal cybersecurity policy, performance, and threats. Trevor and his team led the successful White House 30-Day Cybersecurity Sprint, produced the Federal Government's Cybersecurity Strategy and Implementation Plan (CSIP), and architected the President's Cybersecurity National Action Plan (CNAP).

10:10 am – 10:50 am	**NIST Computer Security Division (CSD) and Applied Cybersecurity Division (ACD) Updates:** Matthew Scholl, Division Chief, CSD and Kevin Stine, Division Chief, ACD

Matt Scholl is the Division Chief of the NIST Computer Security Division and his publications include SP 800-88 and SP 800-30-1. Prior to Joining NIST Mr. Scholl was a commander in the US Army Infantry and Armored Cavalry serving in several positions both overseas and in the continental United States. After leaving the military he was a Configuration Manager and Quality Assurance Specialist for software development safety of flight systems. Mr. Scholl also worked as a contractor designing and developing systems for the USDA, and DOD. Most recently he worked in several federal agencies providing support for FISMA compliance programs and conducting operational security from policy development to technical implementations and assessments.

Matt Scholl is a CISSP and a certified ISO 9000:2000 Quality System Auditor. Matt Scholl has History and Computer Science degrees from the University of Richmond and a Masters of Information Systems from the University of Maryland.

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.

10:50 am – 11:00 am	**Break**
11:00 am – 11:30 am	**Federal CIO Council Update:** Craig Jennings, Senior Advisor, Federal CIO Council

Craig Jennings is Senior Advisor to the Federal CIO Council. In that role, he manages the operations of the Council; coordinates government-wide technology policy between OMB, Federal Agency CIOs, and other government offices; and manages Council working groups.

Before joining the Federal Government in 2013, Craig was Manager of Federal Spending and Contracting Policy at the Center for Effective Government (CEG, formerly OMB Watch). Craig started working for OMB Watch in 2006 while completing his master's degree in public policy at American University. At OMB Watch, Craig advocated for increased transparency and oversight of Federal spending and helped implement FedSpending.org, an online searchable database of Federal contracts and grants spending.

Prior to working for OMB Watch, Craig was an IT consultant in Texas. Craig consulted for KPMG, EnForm Technology, and Sungard Consulting, focusing on web development and business process change management.

Craig holds an M.P.P. from American University and a B.B.A. from the University of Texas at Austin.

11:30 am – 12:30 pm	**Lunch – West Square** Attendees may go through the regular NIST cafeteria line and pay on their own. Cash or credit is accepted. Seating in the West Square is reserved for our group or you may go to the outside courtyard. You can order sandwiches on one side or select from the premade entries in the middle, or salad bar. Sandwiches are priced separately. The other food items are weighed at the cash register. You can go offsite and return by showing your conference badge and photo ID to the guards when coming through the gates. You do not need to go into the Visitor Center.

12:30 pm – 1:15 pm	**Establishing a Tier 2 Information Security Risk Management Program: How a department-wide security gap analysis provided basis for new security program:** Debra Graul, Information Systems Security Manager (ISSM), Pension Benefit Guaranty Corporation (PBGC) Office of Benefits Administration (OBA), and Taryne McDonald, Information Owner (IO), PBGC

Debra Graul is an information systems security manager at the Pension Benefit Guaranty Corporation's Office of Benefits Administration. In this role since 2014, she established the department's first holistic Information Security Risk Management Program based on the National Institute of Standards and Technology's Risk Management Framework. Debbie lead a department-wide information security gap analysis that provided quantified measurements of the current state, provided recommendations for identified findings, and developed an action plan to improve the security stance of OBA. Using her experience as a project manager, she helped form the team that worked to establish a Tier 2 security program based on quantified measurements and residual risk metrics to support decision making and risk mitigation strategies for the program.

Debbie is a project management professional and certified authorization professional. She earned a master's degree in applied mathematics from the University of Central Florida.

She has worked at PBGC for the last 20 years, starting as a pension actuary and transitioning to information technology as a project manager. She helped establish an agency-wide community of practice for project management professionals and cultivated a culture of project management at PBGC. She is now serving as a security leader helping to bridge the gap between operations, technology and information security.

Taryne McDonald is an information owner at the Pension Benefit Guaranty Corporation for the Office of Benefits Administration. Taryne manages all security issues associated with the protection of PBGC information for the systems that she oversees, to include coordination for vulnerability scanning, security reviews of third party vendors, and system development planning for POA&M remediation. Taryne has also served as both an ISSO and SA&A Lead for the agency's Enterprise Cybersecurity Division.

Prior to her time at PBGC, Taryne served as the configuration management lead for the Internal Revenue Service. Although a federal employee, Taryne has spent most of her professional career serving as a contractor ISSO for Military Health Systems Tricare Medical Association, where she specialized in DIACAP and DITSCAP control assessments and system accreditation.

Taryne is CISSP certified. She has a master's degree in information systems from the University of Maryland University College.

1:15 pm – 2:00 pm	**Government Accountability Office (GAO) Information Security Update:** Nicholas (Nick) H. Marinos, Assistant Director of Information Security Issues, GAO and Tom Johnson, Senior Information Technology Analyst, GAO

Nick Marinos joined the U.S. Government Accountability Office (GAO) in 2002 and has served as an assistant director within GAO's information technology audit team since 2011. As part of his responsibilities in this role, Mr. Marinos manages multiple audit teams that perform government wide and agency-specific information security and privacy reviews across all major federal agencies. Mr. Marinos is a certified information privacy professional and holds a Master's in Business Administration and a Bachelor's of Science from Virginia Tech.

Tom Johnson joined the U.S. Government Accountability Office (GAO) in 2008 and is a Senior Information Technology Analyst within GAO's information security issues team. As part of his responsibilities, Mr. Johnson manages audit teams that assess information security and privacy controls across the federal government. Prior to entering federal service, he was an IT manager for the state of New York. Mr. Johnson is a certified penetration tester, intrusion analyst and holds a Master's in Public Administration from Rockefeller College and a Bachelor's in Computer Science from the University at Albany.

2:00 pm – 2:15 pm	**Break** (cafeteria closes at 3:00)
2:15 pm – 3:00 pm	**Internet Tradecraft:** Russ Haynal, Expert Internet Instructor & Speaker, Information Navigators

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

Note: Russ Haynal's slides will *not* be posted but he will email them to those that request them. He will also create a web page called http://navigators.com/fcsm.html.

3:00 pm – 3:30 pm	**SP 800-150, *Guide to Cyber Threat Information Sharing:*** Christopher (Chris) Johnson, Senior Computer Scientist, NIST

Chris Johnson is a senior computer scientist in the Security Components and Mechanisms Group within the National Institute of Standards and Technology (NIST) Computer Security Division. His projects include research in cyber threat information sharing, security automation, and software assurance. Prior to joining NIST, Chris worked as a contractor to government agencies and to private sector companies in the financial, insurance, and aerospace sectors in the areas of security and systems engineering, and software development.

3:30 pm – 4:00 pm	**SP 800-184, *Guide for Cyber Event Recovery*:** Jeffrey (Jeff) Cichonski, NIST

Jeff Cichonski is an Information Technology Specialist working with a broad array of technologies at the National Institute of Standards and Technology; working in the Applied Cybersecurity Division under the umbrella of the Information Technology Laboratory. One of his current areas of focus is effectively recovering from a major Cybersecurity event. Other areas of focus include cybersecurity for industrial control systems security, derived credential research, and LTE network security, with a specific interest in security for public safety LTE Implementations. He has a Bachelor of Science in Information Science and Technology from the Pennsylvania State University.

4:00 pm – 4:30 pm	**NIST SP 800-171, *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations:*** Kelley Dempsey, Senior Information Security Specialist, Computer Security Division, NIST

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

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

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

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

Wednesday, August 17, 2016

9:00 am – 9:45 am	**Continuous Diagnostics and Mitigation (CDM):** Willie D. Crenshaw, Jr., Program Executive, National Aeronautics and Space Administration (NASA)

Willie D. Crenshaw, Jr. is a Program Executive in the Office of the CIO at NASA in Washington, D.C. since April 2012. He serves as the Service Executive for the agency Governance, Risk Management, CDM and Threat Management programs that support NASA's cyber security operations. As Service Executive for GR&C, he actively leads the development of programs and projects that continues to transform, enhance and strengthen the NASA IT Cyber security environment.

In 2007-2012 he was with the US Department of Transportation (USDOT). He spearheaded the development and implementation of the FRA's Cyber Security Program, which identified near and long term security, continuous monitoring, and training initiatives. He ensured that existing and emerging e-Gov and CIO mandates from the Office of Management and Budget (OMB), DOT, and FRA were met and that the agency supported the President's Cyber security agenda. He ensured compliance with DOT and OMB Line of Business initiatives and worked closely with the FRA CIO, IT Director and IT Operations Team Lead in ensuring awareness of and compliance with Cyber Security mandates, emerging technologies and mobile device security.

Mr. Crenshaw received his Bachelors in Business Administration and Management from Virginia State University.

9:45 am – 10:15 am	**The New A-130 Policy**: Carol Bales, Senior Policy Analyst, Office of Management and Budget (OMB)

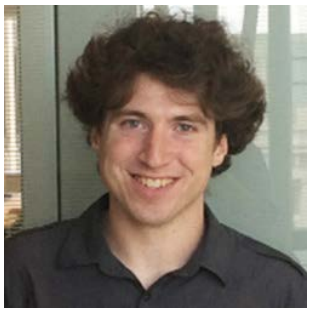
Note: Carol Bales photo and bio were extracted from LinkedIn.

Carol Bales is a Senior Policy Analyst with OMB. She has served in a variety of IT roles and have overseen a number of government-wide initiatives – to include Homeland Security Presidential Directive 12 and the Federal government's transition to IPv6. She currently serves as a member of the Cybersecurity and National Security Unit within the Office of the Federal Chief Information Officer. Her primary focus is on developing cybersecurity policies and providing oversight of Federal cybersecurity initiatives, such as the Federal Risk and Authorization Management Program (FedRAMP). With respect to policy development, she led the revision process for OMB Circular A-130, "Managing Information as a Strategic Resource", and serves as the lead author for this government-wide policy on information technology and information resources management. Ms. Bales assists the Federal Chief Information Officer in overseeing the implementation of information technology throughout the Federal government including advising senior OMB officials on the performance of IT investments and government-wide programs.

Carol Bales served as the Deputy Associate CIO for Cyber Security at the Department of Energy before OMB. Prior to that she was Chief of the Management Information & Security Branch at the Department of Justice.

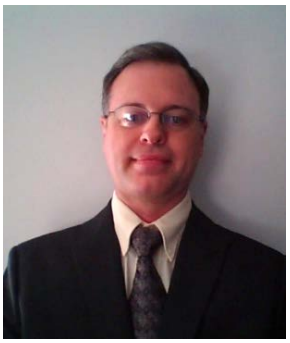
She received a B.S., Information Systems, from the University of Maryland and an M.S., Information Technology, from the University of Maryland University College's Graduate School of Management and Technology.

10:15 am – 10:30 am	Break
10:30 am – 11:00 am	**Migrating the Federal Government to HTTPS:** Eric Mill, General Services Administration (GSA)



Eric Mill is an engineer at 18F, an office of the U.S. General Services Administration that provides in-house technology services for the federal government. Eric's work at 18F focuses on privacy, security, and open government. Previously, Eric was an engineer at the Sunlight Foundation, a non-profit dedicated to government transparency, where he worked on open data infrastructure and policy.

11:00 am – 11:30 am	**Security Beyond A "System" – Fiscal Service's Approach to External Services:** Jim McLaughlin, Manager, Security Policy & Risk Management, Bureau of the Fiscal Service, U.S. Department of the Treasury



Jim McLaughlin is the Manager of Security Policy and Risk Management at the US Treasury's Bureau of the Fiscal Service. He is responsible for development, maintenance, publication, interpretation, and advisory services on security policy matters. Jim is also responsible for security risk management functions such as risk data analytics at Fiscal Service. Jim was the Chief Information Security Officer (CISO) at the Bureau of the Public Debt before Fiscal Service was created by consolidating Public Debt and the Financial Management Service.

Prior to joining Public Debt, Jim worked in various engineering and management roles in the petroleum industry. He was responsible for work such as calculating oil and gas reserves, SEC reporting, developing computer simulations to predict and optimize production for oil and gas fields in the Gulf of Mexico, data acquisition and analysis, cash flow investment projections, and process quality improvement initiatives.

Jim has a degree in Petroleum Engineering from Marietta College and is a CISSP.

11:30 am – 12:45 pm	**Lunch** We do not have the West Square room but you may sit anywhere in the cafeteria or in the outside courtyard. You have the option to go off campus and return by showing your conference badge and photo ID.

12:45 pm – 1:30 pm	**Case Study: Boundary Consolidation to support more efficient, effective use of resources and increased maturity in continuous monitoring:** LaCountiss Hopkins, Information System Owner (ISO), PBGC OBA and Baan Alsinawi, Information Systems Security Officer (ISSO), PBGC/Tala Tek LLC

LaCountiss Hopkins is an information system owner in the Office of Benefits Administration for the Pension Benefit Guaranty Corporation. As the ISO, she oversees security needs of the department. This includes procurement, development, integration, modification, operation, maintenance and disposal, of a major boundary, which consists of 13 major components, server and client level applications, along with a host of tools and services.

LaCountiss is a project management professional and contracting officer's representative level II category. She earned her master's degree in mathematics from George Mason University. While working at PBGC for over 15 years, she served as an actuary calculating defined benefit pension plans and pension liabilities. She also served as a management analyst and managed IT projects through the IT Systems Life Cycle Methodology. She then moved to her role in security.

Baan Alsinawi is the president and owner of TalaTek LLC., a compliance and risk management firm. Baan provides support to the Pension Benefit Guaranty Corporation's Office of Benefits Administration as an information systems security officer. In her role as ISSO, she ensures the implementation of system-level security controls, assists in the determination of an appropriate level of security commensurate with the impact level, participates in self-assessment of system safeguards and program elements and in certification and accreditation of the system. She has supported PBGC in security risk management covering both internal and third-party systems, and helped establish OBA's first Tier 2 security program.

Baan is a member of ISC2, and is CISSP and ITIL certified. She has more than two decades of experience in information technology and has served in various capacities from managing networks and software sales to directing security operations.

1:30 pm – 2:00 pm	**Lessons Learned from FedRAMP:** Claudio Belloli, Program Manager for Cybersecurity, FedRAMP PMO, General Services Administration (GSA)

Claudio Belloli joined the FedRAMP team in July 2014 as the Program Manager for Cybersecurity. In that role, Claudio oversees all of the cloud service providers (CSPs) going through the JAB P-ATO authorization process. He manages the PMO's ISSO team and serves as the primary liaison to the JAB CIO's Technical Representatives and their review teams. Claudio is responsible for ensuring authorization packages meet the rigorous reviews set forward by the JAB and that vendors with JAB P-ATO continue to maintain their authorizations through Continuous Monitoring.

Claudio previously worked for Booz Allen Hamilton, where he served as the lead cloud security advisor supporting the DOD CIO. He was an original member of the DOD JAB technical review teams for the first FedRAMP provisional ATOs in 2012. He will continue to bring his cybersecurity and cloud expertise as FedRAMP expands the CSPs we authorize through the JAB.

2:00 pm – 2:15 pm	**Break** (cafeteria closes at 3:00)
2:15 pm – 2:30 pm	**Speak Out – sign up at the conference registration desk (5 minutes per person)**

2:30 pm – 3:00 pm	**Continuous Diagnostics and Mitigation (CDM) Update, Interagency Communications, and Agency Involvement:** Susan Hansche, Training Manager, Federal Network Resilience, US Department of Homeland Security (DHS)

Susan Hansche, CISSP-ISSEP, is the Training Manager in the Federal Network Resilience office at the Department of Homeland Security. She has over 20 years of experience in the training field and specific expertise in designing, developing, and implementing Information Assurance and Cybersecurity training programs for Federal agencies. For the past 17 years the focus of her professional experience has been with information system security and building training programs that provide organizations with the skills necessary to protect their information technology infrastructures. An additional expertise is in the understanding of the Federal information system security laws, regulations, and guidance required of Federal agencies. She is the lead author of "The Official (ISC)2 Guide to the CISSP Exam" (2004), which is a reference for professionals in the information system security field studying for the Certified Information System Security Professional (CISSP) exam. Her second book "The Official (ISC)2 Guide to the ISSEP CBK" (2006) is a comprehensive guide to the Information Systems Security Engineering Model for designing and developing secure information systems within the federal government. Ms. Hansche has written numerous articles on information system security and training topics and has given many presentations at conferences and seminars.

3:00 pm – 3:30 pm	**DHS Cybersecurity National Action Plan (CNAP) Activities & DHS Binding Operational Directives (BODs):** Nancy Lim, FNR Senior Advisor and CS&C Principal Liaison to OMB Cyber and National Security Unit, U.S. Department of Homeland Security

"Nancy" Myoung-Sook Lim joined the Federal Network Resilience (FNR) Division under the Office of Cyber Security & Communications (CS&C) for the Department of Homeland Security (DHS) in November of 2014. She presently serves as the Senior FNR Advisor and the Principal CS&C Liaison to OMB Cyber & National Security Unit on all aspect of Cybersecurity, and implementing FISMA 2014. She is responsible for providing executive leadership in various implementation activities and coordination for FISMA 2014 with OMB, NSC, and Department and Agencies.

Ms. Lim presently serves as one of the chairs to the Joint Cybersecurity Performance Management Working Group (JCPMWG) under the Federal CIO Council, Information Security and Identity Management Committee (ISIMC), and Security Program Management Sub-Committee (SPMSC). She previously served as one of the chairs to the Joint Federal Continuous Monitoring Working Group (JCMWG) under Federal CIO Council/ISIMC/SPMSC.

Prior to joining DHS, she served as the Chief Information Security Officer (CISO) and IT Director for the Defense Technical Information Center at the Department of Defense (DOD) from 2012 through 2014. In 2012, she served as the Deputy Associate Chief Information

Officer (DACIO) for USDA's Agriculture Security Operations Center (ASOC). She was responsible for providing executive leadership in security operations, architecture, and risk management, and was responsible for securing USDA networks and systems by collecting, analyzing, integrating and sharing information among the USDA component services. Ms. Lim coordinated cyber-security situational awareness, resources, and reporting for USDA organizations and personnel in order to protect USDA programs, information, & assets.

Prior to joining USDA OCIO leadership team, Ms. Lim served at the Department of Health and Human Services. In her two years of services at HHS, her leadership and executive strategic direction led her to establish and develop the HHS Continuous Monitoring Program with the support of 13 Operation Divisions (OPDIVs). Additionally, she served as a principal advisor and senior technical resource on IT legislation and directions, and advised on the implementation and management of various aspects of IT Security and Privacy programs for the entire Department.

Prior to HHS, she spent over 13 years in international federal IT consulting for the U.S. Department of State supporting various high priority enterprise-wide/department-level programs under the Bureau of Consular Affairs, Bureau of Diplomatic Security, and the Bureau of Information Resource Management.

Ms. Lim received a Bachelor of Science from the College of William and Mary. She has completed Leadership for a Democratic Society at Federal Executive Institute (FEI) in 2012 and Senior Executive Fellows at Harvard Kennedy School Executive Education in 2016. She also holds current professional credentials on information security, Certified Information Systems Security Professional (CISSP).

3:30 pm – 4:15 pm	**The Cybersecurity Strategy and Implementation Plan (CSIP) and FY2016 CIO FISMA Metrics:** Cindy Faith, Cyber Risk Advisor and AISSO, DHS ICE/Contractor

Cindy Faith is an Information Security practitioner with a broad range of technical, business and program skills along with 17 years of experience in cybersecurity consulting, business development, program management, and technical support. Currently, she works for Deloitte and serves as an ISSO dedicated to an information system which has all the attendant security issues associated with legacy systems. She operates as principal advisor to the system owner on all matters involving security and FISMA/RMF compliance while playing whack-a-mole with new vulnerabilities that pop up regularly. She has a broad understanding of cybersecurity risk management and is also acutely aware of the pressing need to develop quantitative cybersecurity risk assessment methods.

Cindy is a member of ISSA RMF SIG, ISACA, and chairs the Regulatory & Policy group for the InfraGard National Capital Region (NCR). She can be found on LinkedIn for more background info.

4:15 pm – 4:20 pm	**Closing:** Pat Toth, NIST

Federal Computer Security Managers' Forum

Website: http://csrc.nist.gov/organizations/cspmf.html

The August 16-17 conference presentations, receiving permission, will be posted under Events. http://csrc.nist.gov/groups/SMA/forum/events.html

The fcsm@nist.gov list serve is an informal group sponsored by NIST to promote the sharing of information system security information among federal agencies. Participation in the listserv is open to federal government employees who participate in the management of their organization's information system security program; exceptions have been made. To join, email: sec-forum@nist.gov. You need a .gov or .mil email address.

Half day meetings are held every other month and once a year, a two day "Offsite" is held. The two day "Offsite" used to be held away from NIST. Meeting announcements are made through the list serve. Topic suggestions and volunteer presenters are welcome.

Pat Toth is the Chairperson and Peggy Himes assists with administrative matters. Contact: patricia.toth@nist.gov, 301-975-5140 or peggy.himes@nist.gov, 301-975-2489.