Federal Computer Security Managers' Forum

NIST – August 26-27, 2015

Program

Wednesday, August 26, 2015

Welcome: **Patricia Toth, National Institute of Standards and Technology (NIST), Forum Chairperson**

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

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

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

NIST Computer Security Division Update: **Matthew Scholl, NIST, Computer Security Division Chief**

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.

How to Best Protect Against Future Attacks: **Trevor H. Rudolph, Office of Management and Budget (OMB), Chief, Cyber and National Security Unit (OMB Cyber)**

Trevor H. Rudolph is the Chief of OMB's Cyber and National Security Unit (OMB Cyber). In this role, Trevor is responsible for advising the U.S. Chief Information Officer and White House leadership on Federal cybersecurity policy, programs, and threats. Trevor is building OMB's first ever dedicated cybersecurity unit tasked with strengthening Federal cybersecurity through data-driven oversight and policy implementation. The OMB Cyber Unit is comprised of cybersecurity technical and policy experts with over 50 years of combined experience.

Implementing TIC E^{3}A in Government and Using the XLA Threat Reduction and Correlation Tool (xTract^{TM}): **Sandra Paul-Blanc, National Archives & Records Administration (NARA), Chief IT Security Officer (CISO) and Philip Kulp, XLA, Senior Information Security Architect**

Sandra Paul-Blanc will present factual information on how NARA has been able to successfully implement E3A (challenges and success). Phil Kulp (XLA) will present a demo of xTract.

Sandra Paul-Blanc, CISSP, is CISO at NARA. Prior to NARA, she was with the Department of Treasury, the Department of Defense, and the Intelligence Community. She received her Masters of Information System from the University of Phoenix and a Certification in Executive Leadership from Cornell University from 2008-2009.

Philip Kulp has been a security consultant at XLA working with the National Archives and Records Administration, since 2008. He has developed several automated tools which assist with centralized vulnerability reporting and integrations of feeds from multiples data sources. While at NARA, Philip has also assisted the agency with developing a continuous monitoring strategy, investigating potential compromises and writing white papers for integrating a security architecture into the enterprise. Philip earned his Master's in Electronic Commerce from the University of Maryland, University College in 2007. His most recent work is developing an automated solution to parse, store and generate extended metadata from the DHS EINSTEIN 3A (E3A) program.

The xTract tool was developed in response to the new stream of data coming from E3A, which requires an automated solution to handle the potentially hundreds or thousands of notices per day. E3A resides outside the agency network and therefor has limited vision into the assets connected to the internal network. xTract extends the capability of E3A into the internal network by correlating the notices with log data to identify the assets or people associated with the notice and provides sufficient information for a security analyst to act on the threat.

Federal Computer Security Managers' Forum website: http://csrc.nist.gov/organizations/cspmf.html The August 26-27conference presentations receiving permission will be posted under Events.

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 only open to federal government employees who participate in the management of their organization's information system security program. Email to join: sec-forum@nist.gov.

GAO Information Security Update: **Gregory C. Wilshusen, Government Accountability Office, Director Information Security Issues**

Greg Wilshusen has nearly three decades of auditing, financial management and information systems experience. Before joining the GAO in 1997, Wilshusen held a number of public and private-sector positions, including senior systems analyst at the Department of Education. He also served as the controller for the North Carolina Department of Environment, Health and Natural Resources, and held senior auditing positions at Irving Burton Associates, a professional and technical services firm, and with the U.S. Army Audit Agency.

He's a certified public accountant, certified internal auditor and certified information systems auditor. Wilshusen earned a Bachelor of Science degree in business administration/accounting from the University of Missouri and a Master of Science degree in information management from George Washington University's School of Engineering and Applied Sciences.

NIST SP 800-163, *Vetting the Security of Mobile Applications*: **Steve Quirolgico, NIST, Computer Security Division, Computer Scientist**

Steve Quirolgico is a Computer Scientist with the NIST Computer Security Division. He is the principle author of NIST Special Publication 800-163, Vetting the Security of Mobile Applications, and architect of the NIST AppVet mobile application vetting system and DARPA TransApps App Testing Portal. For his work in mobile application security, he received the 2013 Department of Commerce Gold Medal and 2014 Government Computer News (GCN) Awards. Prior to joining the Computer Security Division, Dr. Quirolgico worked in the NIST Advanced Network Technologies Division where he received the 2008 Department of Commerce Gold Medal Award for his work in wireless interoperability of public safety communications systems. He was also awarded U.S. patent 6845084 for his work in ad hoc network routing protocols. He holds an M.S. from Drexel University and Ph.D. from the University of Maryland, Baltimore County.

Using Risk Management to Improve Privacy in Information Systems: **Ellen Nadeau, NIST, Cyber Policy Strategist**

Ellen Nadeau is a Cyber Policy Strategist at the National Institute of Standards and Technology (NIST), working with the National Program Office to implement the National Strategy for Trusted Identities in Cyberspace (NSTIC). Ellen supports a number of critical programs at NIST, including the new privacy engineering program and the NSTIC pilots program. She plays an integral role in driving various NIST publications from draft to publication, and in developing and maintaining office metrics to assess progress of implementing the NSTIC.

Ellen received her Master's of Public Administration from New York University, where she was a Scholar for Service at the NYU Center for Interdisciplinary Studies in Security and Privacy. She also holds a B.A. in Industrial/Organizational Psychology from The George Washington University. Previously, Ellen worked at a digital rights nonprofit (*Derechos Digitales*) in Santiago, Chile, as a Google Policy Fellow, and with the National Center for Missing & Exploited Children in the Netsmartz Workshop.

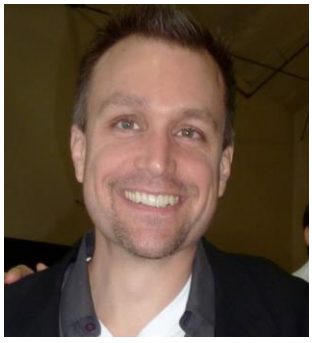
Framework for Improving Critical Infrastructure Cybersecurity: **Matthew Barrett, NIST, Program Manager, NIST Cybersecurity Framework**

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

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

Mobile Application Security and PIV Derived Credentials: **Jane Maples, NASA, Manager of the NASA Center for Internal Mobile Apps (CIMA) and Peter Cauwels, NASA**

Jane Maples is an Information Technology specialist at NASA's Marshall Space Flight Center in Huntsville, Alabama. She manages the Enterprise Service Bus (ESB) Line of Business and the Center for Internal Mobile Applications (CIMA) at the NASA Enterprise Applications Competency Center (NEACC). She led the effort to establish the CIMA services and capabilities (e.g., Dev Center, Pulse analytics, standard login and Secure Mobile Access Point (SMAP) module, several reusable code libraries) as well as the Agency's centralized internal appstore (apps@NASA). She also led the effort to provide an enterprise solution for the implementation, utilization, and management of PIV derived credentials for mobile services utilizing Agency approved ICAM infrastructure and services.

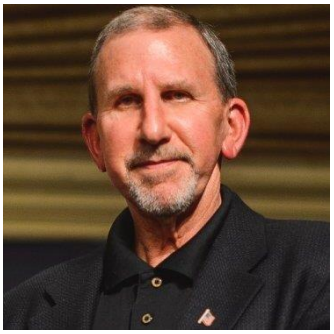


Mr. Peter Cauwels has managed numerous development projects and has extensive knowledge in the areas of enterprise integration, service oriented architecture, and application development. His project experience spans both the public and commercial sectors. Peter has been supporting NASA since 2001. Over the last 10 years at the NASA Enterprise Applications Competency Center, Peter has successfully grown and managed a large team of developers focused on custom software development, web development, mobile development, and software integration at NASA. Peter's strategic vision and leadership of IT resources at NASA secured the successful design, development and implementation of the Open Enterprise Service Bus (ESB) and integration of key NASA enterprise systems.

Peter currently manages the NEACC ESB line of business that provides key infrastructure services for the Agency as well as CIMA (Center for Internal Mobile Apps - https://cima.nasa.gov/).

Thursday, August 27, 2015

Q&A Session on Recent Updates to FISMA Pubs: **Ron Ross, NIST Fellow, Project Leader, Joint Task Force Transformation Initiative**



Ron Ross is a Fellow at the National Institute of Standards and Technology (NIST). His areas of specialization include information security, risk management, security architecture/engineering, and systems resiliency. Dr. Ross leads the Federal Information Security Management Act Implementation Project, which includes the development of security standards and guidelines for the federal government, contractors, and the United States critical information infrastructure. He is the principal architect of the NIST Risk Management Framework and multi-tiered approach that provides a disciplined and structured methodology for integrating the suite of security standards and guidelines into a comprehensive enterprise-wide information security program. Dr. Ross also leads the Joint Task Force, an interagency partnership with the Department of Defense, the Intelligence Community, and the Committee on National Security Systems that developed the Unified Information Security Framework for the federal government.

In addition to his responsibilities at NIST, Dr. Ross also supports the U.S. State Department in its international outreach program for cybersecurity and critical infrastructure protection. He previously served as the Director of the National Information Assurance Partnership, a joint activity of NIST and the National Security Agency and has been a guest lecturer at many universities and colleges across the country. A graduate of the United States Military Academy at West Point, Dr. Ross served in a variety of leadership and technical positions during his twenty-year career in the United States Army. During his military career, Dr. Ross served as a White House aide and as a senior advisor to the Department of the Army. He is a graduate of the Defense Systems Management College and holds both Masters and Ph.D. degrees in Computer Science from the Naval Postgraduate School specializing in artificial intelligence and robotics.

PIV Implementation at FAA: **Myles Roberts, FAA, Manager, FICAM Program**

Myles Roberts is a Project Manager with the Federal Aviation Administration since April 2009. Duties include: Identify trends in the aviation industry, predict new demands for federal services, and formulate long-term strategies to meet them. Manage five-year initiatives for air traffic operations, safety risk, global engagement, and workforce productivity. Author federal policy to meet developing demands and reduce vulnerabilities. Review effectiveness of federal programs, analyze gaps, and evaluate options to increase value.

Manage Cyber Security projects. Draft, implement and measure policies for cyber security, classified information, communications security, facility security, and personnel security. Coordinate Identity Credential and Access Management (ICAM) for over 100,000 users across a federal agency's enterprise. Examine and implement guidance from National Institute of Standards and Technology (NIST) and Office of Management and Budget (OMB). Design Cyber Security architecture for—and manage system development life cycles (SDLC) of—Cyber Security information systems and applications.

Previous experience includes the US Treasury, Potter Anderson & Corroon LLP, and Steptoe & Johnson PLLC. Mr. Roberts is an attorney and member in good standing of California, Delaware, and West Virginia bars. He is a corporate and finance lawyer counseling Delaware corporations on corporate law and governance issues; representing underwriters, issuers, and conduit borrowers as underwriter's counsel or bond counsel.

Education: University of Virginia School of Law, Juris Doctor, Law 2002 – 2005. Thomas Jefferson High School for Science & Technology, Diploma from Fairfax County's competitive magnet school, Computer Systems research. West Virginia University, BA, Economics & Political Science.

Cloud Assessments: **John Connor, NIST, Information Technology Security & Networking Division, CISSP**

John Connor works on internal assessment and authorizations as well as vulnerability and web application scanning at NIST. Additionally is currently heading the assessment and authorization process for cloud computing at NIST as well as consulting on cloud assessment matters to other agencies. Pervious to his now 8 years at NIST John worked as a contractor and consultant to civilian and defense agencies on various IT projects including server administration, web development, database management and IT security. John holds a CISSP certification and has a BS from George Mason University.

National Vulnerability Database (NVD): **Harold Booth, NIST, Computer Scientist**

Harold Booth is a Computer Scientist at the National Institute of Standards and Technology (NIST). Harold is the project lead for the National Vulnerability Database (NVD) and is involved in the development of the Security Automation Program specifications.

DOT Security Program Management Subcommittee' s Information Assurance Policy Working Group (IAPWG): **Kevin Sanchez-Cherry, Department of Transportation Cybersecurity Policy, Architecture and Training Lead and Information Assurance Policy Working Group (IAPWG) Founder**

Kevin Sanchez-Cherry, CISSP has been the Cybersecurity Policy, Architecture and Training Lead at the US Department of Transportation (DOT) since October 2014. He serves as subject matter expert in, and provides leadership of, and direct responsibility for cybersecurity and information assurance policy and guidance, planning, architecture, training, education, and cybersecurity workforce development.

As the Cybersecurity Policy Lead, he directs a team in assessing the need for new or updated policies and guidance based upon: evolving business requirements; new initiatives; risks, threats, and identified weaknesses; audit findings and recommendations; and new policies and guidance from authoritative sources such as OMB, DHS, DoD, the Office of Personnel Management (OPM), NIST, and other DOT offices. Kevin also represents DOT on inter-agency policy working groups, subcommittees, and teams, as a subject-matter-expert in cybersecurity and information assurance policy, recommending or providing input into activities and contributing to the development of deliverables that are produced to ensure that they support the DOT mission and business, reflect DOT interests, and implement security best practices.

He plans, develops and implements training on DOT cybersecurity and information assurance policies and guidance to familiarize DOT cybersecurity personnel, executives, and general employees with requirements, roles, responsibilities, and implementation timelines. He provides input into DOT Workforce Development and Planning initiatives, representing the OCISO and cybersecurity staff as the DOT Cybersecurity Training Lead.

As the Cybersecurity Architecture Lead, Kevin represents the Office of the Chief Information Security Officer (OCISO) on working groups and task forces to ensure adequate security is built into and implemented in DOT systems and networks. He has contributed to the DOT Chief Technology Officer's (CTOs) Cloud Strategy, currently in draft.

Kevin is also the Founder and Co-Chair of the Information Assurance Policy Working Group (IAPWG). The Working Group

provides Federal interagency coordination and cooperation in the development 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. Prior to the DOT, Kevin was the Information Assurance Policy Lead for the US Department of Education, Certification & Accreditation Program Manager for the US Secret Service and a contract IT Security Specialist at NARA, DOD, Veterans Affairs, and DOJ Anti-Trust Division.

Speak Out – If you would like to share; sign up at registration desk.

- **Daniel Wood, Treasury – PKI Landscape Terminology**
- **Pat Toth - fcsm@nist.gov listserve**

IT Policy Initiatives: **Adam Sedgewick, NIST, Senior Information Technology Policy Advisor**

Adam Sedgewick serves as Senior Information Technology Policy Advisor at the National Institute of Standards and Technology. In this role, Adam represents NIST on the Department of Commerce's Internet Policy Task Force and advises NIST leadership on cybersecurity issues. Previously, Adam was Senior Advisor to the Federal Chief Information Officer Council, developing and coordinating cross-agency initiatives and assisting in the implementation of governmentwide policy.

Adam served as Professional Staff Member for the Senate Committee on Homeland Security and Governmental Affairs for nine years, handling cyber security and federal information technology policy. In 2008 and 2013, Sedgewick received the Fed 100 award for his contributions to the Federal information technology community and both BankInfoSecurity and GovInfoSecurity named Sedgewick a "Top Ten Influencer" for 2014. He was also awarded the 2014 AFCEA Government-Wide Initiatives Excellence Awards for Security, and was named one of Security Magazine's Most Influential People in Security for 2014. Adam is a graduate of Princeton University.

Census Risk Management Program Implementation: **Jaime Lynn Noble, US Census Bureau, CAP Assistant Division Chief for Policy & Compliance, Office of Information Security**

Jaime Noble became the Deputy Chief Information Security Officer & Risk Management Program Manager at US Census Bureau in October 2012. She began her career at Census in 2001 as a programmer supporting Demographic surveys and censuses. In 2008, she moved to the Office of Information Security (OIS) and led the Bureau's transition from the Certification & Accreditation Process to the Risk Management Framework. Today, she is responsible for Security Engineering, initial and on-going Security Assessments and Security Status Reporting supporting On-going Authorization as she continues to improve the Bureau's Information security risk management program and ensure information systems are in compliance with federal information security requirements. In 2014, Jaime and her team received the Department of Commerce Gold Medal Honor Award for developing an innovative security program that allows executives to better understand risk and determine the most cost-effective actions to manage them while minimizing the impact on the mission.

Jaime is a Certified Authorization Professional (CAP), has a Bachelor's Degree in Management Science & Information Systems from the Pennsylvania State University and a Master's Certificate in IT Project Management from the George Washington University.

Department of Homeland Security (DHS) Continuous Diagnostics and Mitigation (CDM) Program Overview: **Martin Stanley, U.S. Department of Homeland Security, Office of Cybersecurity and Communications, Cybersecurity Assurance Branch Chief – Federal Network Resilience**

Martin Stanley is the Branch Chief of the Cybersecurity Assurance Branch and the Cybersecurity Performance Management Branch at Office of Cybersecurity and Communications at the Department of Homeland Security. In this role Martin leads the assessment and reporting of civilian federal agency cybersecurity programs and performance under FISMA. While at DHS Martin has led the development of the CDM Phase II technical requirements and serves as the co-chair of the Information Security Continuous Monitoring sub-working group of the Federal CIO Council. Martin previously led the Information Security Program at the Food and Drug Administration where he oversaw world-wide enterprise information security for 300+ applications and 2 modern data centers serving 17000+ employees and contractors. Prior to his federal service Martin held executive leadership positions at Vonage and UUNET Technologies.

Education: William & Mary - B.S., Physics

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/

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.

Also on the CSRC site:

- Federal Information Processing Standards (FIPS): security standards;
- NIST Special Publications (SPs): explained above;
- NIST Interagency or Internal 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.