Federal Computer Security Managers' Forum Annual Offsite

Program and Speaker Profiles

NIST Green Auditorium

May 15-16, 2018

National Institute of Standards and Technology
U.S. Department of Commerce

Tuesday, May 15, 2018

9:00 – 9:05 am	**Forum Welcome and Day 1 Overview**
Victoria Yan Pillitteri, Forum Co-Chairperson, Computer Security Division, NIST Ms. Pillitteri will cover the agenda and logistics for the Offsite.	
9:05 – 9:25 am	**Welcome to NIST and Event Overview**
Charles H. Romine, Ph.D., Director, Information Technology Laboratory, NIST Dr. Romaine will provide welcoming introductions to NIST.	
9:25 – 10:00 am	**FISMA – Yesterday, Today and Tomorrow**
Tammy L. Whitcomb, Acting Inspector General for the U.S. Postal Service Office of Inspector General and Council of the Inspectors General on Integrity and Efficiency (CIGIE) Information Technology Committee Chair Ms. Whitcomb will discuss how the Federal Information Security Modernization Act (FISMA) of 2014 requires the head of each Federal agency to provide information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems. Additionally, FISMA requires agency heads to report on the adequacy and effectiveness of the information security policies, procedures, and practices of their enterprise. The Inspectors General (IG) are uniquely positioned to conduct audits of host agencies, both because of deep knowledge of agency systems and robust auditing experience.	
10:00 – 10:30 am	**Update from the Office of Management and Budget**
Taylor C. Roberts, Cybersecurity Advisor, Cyber and National Security Unit, Office of the Federal Chief Information Officer, Office of Management and Budget Mr. Roberts will provide an update on the work that the Office of the Federal Chief Information Officer is doing in relation to the President's Management Agenda and the IT Modernization effort.	
10:30 – 10:45 am	**Break**
10:45 – 11:30 am	**FY 2018 FISMA Metrics**
Craig Chase, IT Security Program Manager, Office of Cybersecurity and Communications, Federal Network Resilience, Department of Homeland Security Mr. Chase will discuss how the current Federal Information Security Modernization Act (FISMA) metrics are used to measure cybersecurity program performance effectiveness across the Federal Agencies and how those metrics feed into the FISMA Report to Congress. Furthermore, he will present where the FISMA metrics are going in FY 2019 and beyond as they mature beyond the current model.	
11:30 am – 12:15 pm	**Security Architecture Review**
Alan McClelland, Deputy Branch Chief, Federal Network Resilience, Department of Homeland Security Mr. McClelland will present DHS' high-level update on their High Value Assets (HVA) Program. This update will include the HVA Strategic plan, Security Architecture Review (SAR) processes, Risk and Vulnerability Assessments (RVA) processes, Future enhancements, HVA Control Overlay, and HVA data calls.	
12:15 – 1:15 pm	**Lunch**

Tuesday, May 15, 2018 (cont.)

1:15 – 2:45 pm	**Information Security at the VA: Perspectives from Office of Information & Technology and Office of the Inspector General**
Mike Bowman, Director, Information Technology and Security Audits, Department of Veterans Affairs (VA) Office of the Inspector General **Dominic Cussatt, Deputy Chief Information Officer for Information Security & Chief Information Security Officer, VA** Mr. Cussatt will speak on the Office of Information Security's (OIS) efforts to transition VA to the Enterprise Cybersecurity Strategy Program (ECSP) and align VA with Federal guidelines, specifically the National Institute of Standards and Technology (NIST) Risk Management Framework (RMF) and Cybersecurity Framework (CSF). Mr. Bowman will speak on standard practices the Office of Inspector General utilizes to coordinate and conduct the annual audit of VA's Information Security Program in accordance with the Federal Information Security Modernization Act.	
2:45 – 3:00 pm	**Break**
3:00 – 3:30 pm	**Update from the U.S. Government Accountability Office**
Nick Marinos, Director, Cybersecurity and Information Management Issues, U.S. Government Accountability Office Mr. Marinos will provide an update on the activities and publications of the Government Accountability Office. This presentation will address key issues related to information security and cybersecurity and highlight current GAO key initiatives.	
3:30 – 4:15 pm	**NIST SP 800-37 Rev. 2 and NIST SP 800-53 Rev. 5 Update**
Kelley Dempsey, Senior Information Security Specialist, Computer Security Division, NIST **Naomi Lefkovitz, Senior Privacy Policy Analyst, Program Manager, Privacy Engineering Program, Applied Cybersecurity Division, NIST** Ms. Dempsey and Ms. Lefkovitz will provide an update on NIST SP 800-37 Rev. 2 *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy (Discussion Draft)* and NIST SP 800-53 Rev. 5 *Security and Privacy Controls for Information Systems and Organizations.*	

Wednesday, May 16, 2018

9:00 – 9:05 am	**Forum Welcome and Day 2 Overview**
Jody Jacobs, Forum Co-Chairperson, Computer Security Division, NIST Ms. Jacobs will give an overview of today's schedule.	
9:05 – 9:20 am	**Overview and Update: NIST Computer Security Division and Applied Cybersecurity Division**
Matt Scholl, Computer Security Division Chief, NIST **Kevin Stine, Applied Cybersecurity Division Chief, NIST** Mr. Scholl and Mr. Stine will provide an update on the activities and publications of the Computer Security Division and Applied Cybersecurity Division.	
9:20 – 10:15 am	**Next Generation Cybersecurity and Risk Management Guidance—2018 and Beyond**
Ron Ross, NIST Fellow, Computer Security Division, NIST For the past year, NIST has been working with the American Technology Council, the Office of Management and Budget, and Federal agencies to respond to the IT Modernization Initiative and to begin the development of the next generation security and privacy risk management standards and guidelines. In this session, Dr. Ross will present NIST's strategic vision for how its standards and guidelines are being modified to align with the Cybersecurity Framework, integrate privacy principles and concepts, provide a closer connection from agency senior leaders to the security and privacy professionals on the front lines, and promote best practices in systems security engineering to help build more trustworthy, secure, and resilient IT components, systems, and services. Status updates on key publications such as NIST 800-37, Revision 2 and NIST 800-53, Revision 5 will be provided as well as the plans to updates the two NIST flagship standards, FIPS 199 and 200.	
10:15 – 10:30 am	**Break**
10:30 – 11:00 am	**Understanding Blockchain**
Andy Regensheid, Mathematician, Computer Security Division, NIST Mr. Regenscheid will discuss how blockchains are tamper-resistant digital ledger systems implemented in a distributed fashion. At its most basic level, they enable a community of users to record transactions in a ledger shared by that community such that no transaction can be changed once published. This talk will provide a high-level technical overview of blockchain technology and its business applications. The purpose is to help the audience understand how blockchains work so that they can be appropriately and usefully applied to business problems.	
11:00 – 11:45 am	**Security Assessment Finding Risk Reviews**
Jim McLaughlin, Manager, Policy and Risk Management, US Treasury - Bureau of the Fiscal Service **Ralph Jones, Security Analyst, Policy and Risk Management, US Treasury - Bureau of the Fiscal Service** Mr. McLaughlin and Mr. Jones will discuss how security assessments require accurate and consistent risk ratings in order to make good authorization decisions. This presentation details Fiscal Service's process of analyzing and adjusting finding risk ratings assigned by security control assessors. Through collection and analysis of risk ratings assigned by multiple security control assessors across various system FIPS 199 impact ratings, operating environments, and various other factors, the process results in "normalized" risk ratings.	
11:45 am – 12:30 pm	**FY 2018 FISMA Metrics – Privacy**
Charles Cutshall, Office of Information and Regulatory Affairs, Office of Management and Budget Mr. Cutshall will present on OMB's policy and oversight role and authorities with respect to Federal privacy practices and how FISMA reporting supports OMB's policy and oversight objectives. In addition, he will present on the evolution of FISMA Senior Agency Official for Privacy (SAOP) metrics and what Federal agencies can expect to see for FY 2018.	

Wednesday, May 16, 2018 (cont.)

12:30 – 1:30 pm	**Lunch**
1:30 – 2:15 pm	**Government Cybersecurity Assessment and Risk Tool (GOVCAR)**

Patrick Arvidson, Special Assistant to the Office of the National Manager, Department of Defense

Mr. Arvidson will present on the government Cybersecurity Assessment and Risk Tool. It is a mechanism being used and explored across the government to understand, quantify, and have a better understanding of where risk decision should be applied. There is a trend where dependencies are increasing, missions increasing, and networks are getting larger. The cyber threat level continues to increase as well. While all of these issues continue to increase there is a decline in cybersecurity resources to combat threats. There is a tendency to treat these problems as a one-to-one problem, meaning there is one thing that will resolve all issues. This is rarely ever the case. When it's treated as a one-to-one as opposed to a many-to-many to many problem, a solution based on a single perspective may not be the solution for all concerned. It is more of a tiered approach; meaning, a holistic viewpoint is needed.

2:15 – 2:45 pm	**Cloud Authorization Boundary Guidance**

Matt Goodrich, FedRAMP Director, General Services Administration

Mr. Goodrich will discuss how as agencies move to the cloud, understanding all of the risks of a cloud system can be complicated. More and more cloud solutions are using micro-services and other cloud providers to help deliver functionality to the core service agencies are using. This discussion will provide an overview of how FedRAMP is addressing this issue and how to appropriately scope authorization boundaries for cloud services.

2:45 – 3:15 pm	**Cybersecurity Framework v. 1.1 Update**

Jeff Marron, Cybersecurity Framework Program, Applied Cybersecurity Division, NIST

Mr. Marron will discuss the collaboration creation between industry and government, the Cybersecurity Framework consists of standards, guidelines, and practices to promote the protection of critical infrastructure. The prioritized, flexible, repeatable, and cost-effective approach of the Cybersecurity Framework helps owners and operators of critical infrastructure to manage cybersecurity-related risk. Mr. Marron will be presenting on recent Cybersecurity Framework news, Cybersecurity Framework v1.1 basics, as well as an update to the status of NISTIR 8170.

3:15 – 3:45 pm	**NISTIR 8170 Criticality Analysis Process Model**

Celia Paulsen, IT Security Specialist, Computer Security Division, NIST

Ms. Paulsen will discuss the approach to identify the most important piece of technology in your organization. NIST guidance regularly calls out the importance of performing a criticality analysis. Ms. Paulsen will walk through the process of identifying the most important systems and components in an organization as described in NISTIR 8170.

Patrick Arvidson serves as the Special Assistant to the Office of the National Manager for National Security Systems (NSS) for the National Security Agency (NSA), providing oversight and guidance on Cybersecurity and computer security strategy and requirements to secure NSS. As Chair of a joint working group, NIPR/SIPR CyberSecurity Architecture Review (NSCSAR), he drives development of a framework to categorize threat and reduce risk to manageable levels to enable portfolio management for acquisition and design of computer systems. The Office of The National Manager is directly responsible for all NSS across the government containing classified and/or sensitive information critical to military and intelligence activities. Mr. Arvidson graduated in 2004 from the University of Maryland University College with a Masters of Science in Information Assurance. In 2010 he graduated from the Naval War College in Rhode Island with a Masters of Arts in National Security and Strategic Studies.

Mike Bowman is the Director of the Information Technology and Security Audits Division, Office of Inspector General (OIG) at the Department of Veterans Affairs. As Director, Mr. Bowman supervises the OIG's annual evaluation of the information security program in connection with the Federal Information Security Modernization Act (FISMA). Mr. Bowman has more than 25 years of experience auditing and evaluating system implementation projects, both in the Federal government and in private industry. Prior to joining the VA OIG, Mr. Bowman was the Assistant Director for Management Advisory Services at the U.S. House of Representatives OIG, which performs audits of system implementation projects at the House. Mr. Bowman graduated with honors from the University of Colorado (CU) with a Bachelor of Science degree, while majoring in business administration and accounting. In 1990, the Colorado Society of Certified Public Accountants selected Mr. Bowman as the outstanding accounting graduate from CU. Mr. Bowman is a Certified Public Accountant, a Certified Information Systems Auditor, and a Microsoft Certified System Engineer.

Craig Chase currently serves as a Security Program Manager for CyberScope at the Department of Homeland Security (DHS), Federal Network Resilience (FNR), Cybersecurity Program Management (CPM) Branch. Craig coordinates and leads the development of the Federal Information Security Modernization Act (FISMA) Chief Information Officer (CIO) metrics with OMB and the Federal Agencies, as well as the collection and reporting of all FISMA metrics across the Federal government through the CyberScope reporting application. Craig has over 24 years information technology experience to include 16 years of cybersecurity experience at DHS, Small Business Administration (SBA), United States Department of Agriculture (USDA) and the Department of Commerce (DOC). Craig has a Master's of Science in the Management of Information Technology (MSMIT) from the University of Virginia and is a Certified Information Systems Security Professional.

Charles Cutshall is a member of the Privacy Branch within the Office of Management and Budget (OMB) Office of Information and Regulatory Affairs where he is responsible for developing and overseeing Federal agencies' implementation of Federal privacy policies. Among other things, his portfolio includes OMB Circular A-130, Managing Information as a strategic Resource, and implementing guidance for the Federal Information Security Modernization Act of 2014. Prior to joining OMB, Charlie developed privacy policies for and supported compliance programs at the Department of the Treasury and the Department of Homeland Security.

Dom Cussatt is Deputy CIO for Information Security and CISO, and oversees information security for the VA as it provides services to 22 million US veterans with a $190B annual budget. He provides strategic leadership to a team of cybersecurity specialists who execute VA's cybersecurity program, information security risk management and metrics activities, VA cybersecurity policy and strategy portfolio maintenance, cyber workforce professionalization activities, and the 24/7 operation of the VA Cybersecurity Operations Center (CSOC), all to ensure secure and reliable operation of VA's $4B annual information technology infrastructure supporting the VA mission and over 350,000 users world-wide. Mr. Cussatt has over 25 years of public and private sector IT implementation and oversight experience, and was previously with the US Department of Defence (DoD) CIO' office for 12 years. During his tenure as DoD Deputy CISO for Cybersecurity Policy and Strategy, he oversaw the DoD Cybersecurity Program and was also the Director of the DoD International Cybersecurity Program. In 2014, he was selected by the 28 North Atlantic Treaty Organization (NATO) nations as the National Co-Chair of the NATO Information Assurance/Cyber Defense Capability Panel which is the source for policy development and advice on technical aspects of cyber defence matters within the NATO Alliance. He also served a three and a half year term as Tri-Chair for the Committee on National Security Systems (CNSS) Subcommittee, which provides a national forum to establish minimum security standards and doctrine for US national security systems.

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, NIST SP 800-137, NISTIR 8011, and NISTIR 8023, 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.

Matt Goodrich is the Director for the Federal Risk and Authorization Management Program (FedRAMP) for GSA's Technology Transformation Service (TTS). Matt has worked on FedRAMP as part of the Federal Cloud Computing Initiative since August of 2009. In this role, he manages the FedRAMP Program Management Office (PMO) and sets the overall direction of the program. As a mandatory Federal-wide initiative, FedRAMP is one of the leading cloud computing security programs paving the way for cloud adoption and ensuring the security of cloud computing solutions used by the US Government. During his tenure at OMB, he has authored numerous publications. Matt began his career in the Federal government as a Presidential Management Fellow (PMF) in 2009. Matt has a BBA in Computer Information Systems from the University of Miami (FL) and a Juris Doctor from the University of Denver.

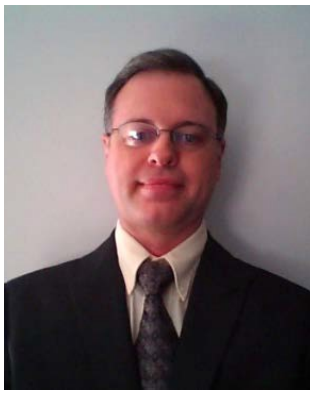
Ralph Jones is a security analyst in Policy and Risk Management at the US Treasury's Bureau of the Fiscal Service. He is responsible for drafting and publishing bureau-wide security policy, conducting risk assessments, analyzing policy and risk metrics, and advising bureau staff regarding implementation of security controls and application of risk management to bureau systems, services, and business processes. Ralph is also responsible for representing Fiscal Service in policy and risk management working groups and government forums. Ralph serves as the co-chair of the Treasury Policy Working Group and is responsible for leading several significant enhancements to the bureau's security policy and risk management practices.

Naomi Lefkovitz is the Senior Privacy Policy Advisor in the Information Technology Lab at the National Institute of Standards and Technology, U.S. Department of Commerce. Her portfolio includes work on the National Strategy for Trusted Identities in Cyberspace (NSTIC), privacy engineering, privacy-enhancing technologies, cybersecurity and standards development. FierceGovernmentIT named Ms. Lefkovitz on their 2013 "Fierce15" list of the most forward-thinking people working within government information technology, and she is a 2014 Federal 100 Awards winner. Before joining NIST, she was the Director for Privacy and Civil Liberties in the Cybersecurity Directorate of the National Security Staff in the Executive Office of the President. Her portfolio included the NSTIC as well as addressing the privacy and civil liberties impact of the Obama Administration's cybersecurity initiatives and programs. Prior to her tenure at the White House, Ms. Lefkovitz was a senior attorney with the Division of Privacy and Identity Protection at the Federal Trade Commission. Her responsibilities focused primarily on policy matters, including legislation, rulemakings, and business and consumer education in the areas of identity theft, data security and privacy. At the outset of her career, she was Assistant General Counsel at CDnow, Inc., an early online music retailer. Ms. Lefkovitz holds a B.A. with honors in French Literature from Bryn Mawr College and a J.D. with honors from Temple University.

Nick Marinos joined the U.S. Government Accountability Office (GAO) in 2002 and serves as Director of Cybersecurity & Information Management issues within its Information Technology team. As part of his responsibilities in this role, Mr. Marinos manages audit teams that perform government wide and agency-specific cybersecurity, privacy, and information management 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.

Jeffrey Marron is an IT Specialist at NIST, working on the Cybersecurity Framework project. He also supports other NIST efforts such as outreach to small- and medium-sized businesses, cybersecurity for the Internet of Things, and smart grid cybersecurity. Prior to joining NIST, Jeff spent over 10 years working in IT Security within the Department of Health and Human Services. Among other things, his work included implementing the Risk Management Framework at the Food and Drug Administration (FDA), specifically via the security testing and evaluation of information systems. Jeff also spent several years at FDA conducting security engineering and integration work. In the more distant past, Jeff was an elementary school teacher of English as a Second Language in Maryland schools.

Alan McClelland is the Deputy Branch Chief, Security Engineering within the Office of Cybersecurity and Communications' Federal Network Resilience Division (FNR). As part of FNR's Cybersecurity Assurance Branch, Alan oversees all aspects of the High-Value Asset Program to include Security Architecture Reviews, cybersecurity engineering engagements, and the HVA Program Management Office. Prior to joining DHS, Alan was the U.S. Food and Drug Administration's (FDA) Chief Information Security Officer and Director of Information Security. He oversaw a team that ensured all aspects of the FDA's information security including a 24x7 Security Operations Center. Before Alan's public service, he worked with multiple contractor agencies providing security consulting services, security engineering, and implementations for numerous federal, DOD and commercial agencies. During this time, he oversaw a team of more than 100 employees as program manager to a $100 million contract to design, procure, implement, and operate a complete end to end security solution for a federal agency. Alan has 30 years of Information Technology experience with a deep technical and governance background that has helped him educate and guide federal agencies in reducing risks to their systems, information, and business mission.



Jim McLaughlin is the Manager of 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.

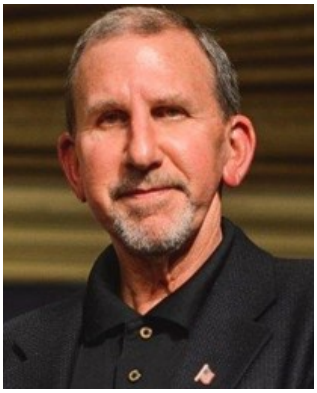
Prior to joining Public Debt, Jim worked in various engineering and management roles in the petroleum industry where he was responsible for work such as calculating oil and gas reserves, SEC reporting, developing computer simulations to predict and optimize production for oil and gas fields in the Gulf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

Celia Paulsen is a cybersecurity researcher and advisor at the National Institute of Standards and Technology (NIST). She develops cybersecurity guidance and helps coordinate policy and research efforts across government, industry, and academic organizations. Her current research focuses on metrics and measures for security, cyber-supply chain risk management, and emerging technologies. She also manages the NIST computer security glossary. In the past, she has researched and developed guidance related to supply chains, replication devices, and small businesses. In addition, she acted as the industry coordinator for the National Initiative for Cybersecurity Education and helped develop that program from its conception. Prior to joining NIST, she was an analyst for the National Security Agency as an enlisted member of the US Army.

Andrew Regenscheid is a mathematician and project lead within the Computer Security Division at the National Institute of Standards and Technology (NIST). As part of the Cryptographic Technology Group, Andrew's focus is on applications of cryptography, including roots of trust, network security protocols, and, more recently, blockchain and distributed ledger technologies.

Charles 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.

Taylor Roberts serves as a Cybersecurity Advisor at the Office of Management and Budget Cyber and National Security Unit within the Executive Office of the President of the United States. Mr. Roberts is responsible for evolving Federal oversight of agency cybersecurity risk management from a compliance effort to a performance-based approach in order to strengthen overall government cybersecurity. To this end, he works together with the Department of Homeland Security, the Intelligence community, Council of Inspectors General on Integrity and Efficiency, and other stakeholders to assess gaps in capability based on current threats and map FISMA metrics to these capabilities to drive performance across the Federal enterprise. Prior to joining the Executive Office of the President, Mr. Roberts served as a Senior Researcher at Oxford University's Global Cybersecurity Capacity Centre. He has also worked at other research institutions researching international strategic dynamics in cyberspace. Mr. Roberts holds a Master of Pacific International Affairs from UC San Diego's School of Global Policy and Strategy and a bachelor's degree in political science from Trinity University.



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.

Matthew Scholl is the Chief of the Computer Security Division in the Information Technology Laboratory at the National Institute of Standards and Technology (NIST). His responsibilities include the Division's cybersecurity strategic direction and planning in Information Technology (IT) research and development, program coordination with other U.S. federal agencies, international engagements, Standards Development Organization strategy and coordination, and internal logistics and operations. In the Computer Security Division, focus areas include measures, metrics and programmatic guidance in information assurance and cybersecurity, cryptography, IT security test and validation, Federal Government agency security programs, creation of reference materials and security primitives and components.

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.

Tammy Whitcomb was appointed as the acting Inspector General for the U.S. Postal Service Office of Inspector General in February 2016. Ms. Whitcomb has served as the Deputy Inspector General since November 2011. In years prior, Tammy served as the Assistant Inspector General for Audit. Tammy came to the Postal Service in November 2005 as an Audit Director. Tammy started her government career at the Internal Revenue Service (IRS) Inspection Service, and transitioned with them as a part of the new Treasury Inspector General for Tax Administration (TIGTA), established in early 1999. During her career at TIGTA, she was an Audit Manager in Dallas, TX for several years before coming to Washington D.C. as the Director of the Office of Management and Policy. Tammy holds a Bachelor's Degree in Accounting and Business Administration from W. J. Bryan College in Dayton, Tennessee and is a Certified Public Accountant, a Certified Internal Auditor, and a Certified Information Systems Auditor.

To our distinguished speakers and panelists,

When planning an event such as the Federal Computer Security Mangers' Forum Annual Offsite, it is imperative to gain the participation of recognized experts across the Federal Government. Thank you for taking time out of your busy schedules to speak at the Forum. Your willingness to share your time and expertise was critical to the success of this years' event.

Thank you!

The NIST Federal Computer Security Managers' Forum Team
Jody Jacobs and Victoria Yan Pillitteri

Thank you

To the following individuals for their help putting this conference together.

- Forum Members for their input on the program and topic ideas.
- NIST Applied Cybersecurity Division and Computer Security Division support:
  - Kevin Stine, Division Chief, Applied Cybersecurity Division (ACD)
  - Matthew Scholl, Division Chief, Computer Security Division (CSD)
  - Patrick O'Reilly and Nikki Keller for website maintenance
- NIST Public Affairs Office Conference Program and Audiovisual Services
  - Gladys Arrisueno
  - Hoyt Cox
  - Akeem Henry
  - Kevin Hill
  - Joe Hynes
  - Mary Lou Norris
  - Crissy Robinson
  - Karen Startsman
- Conference presentations will be posted after the conference to the Forum Website https://csrc.nist.gov/Projects/Forum

The next Forum Quarterly Meeting will be September 10, 2018 at the NIST Gaithersburg, MD Campus in the Heritage Room.

Participation in the Forum Google Group is limited to U.S. federal, state, and local government, higher-education employees and their designated support contractors

To find out how to participate:
https://csrc.nist.gov/Projects/Forum/Forum-Membership