Federal Computer Security Managers' Forum Annual Offsite

Program

NIST Green Auditorium

June 20-21, 2017

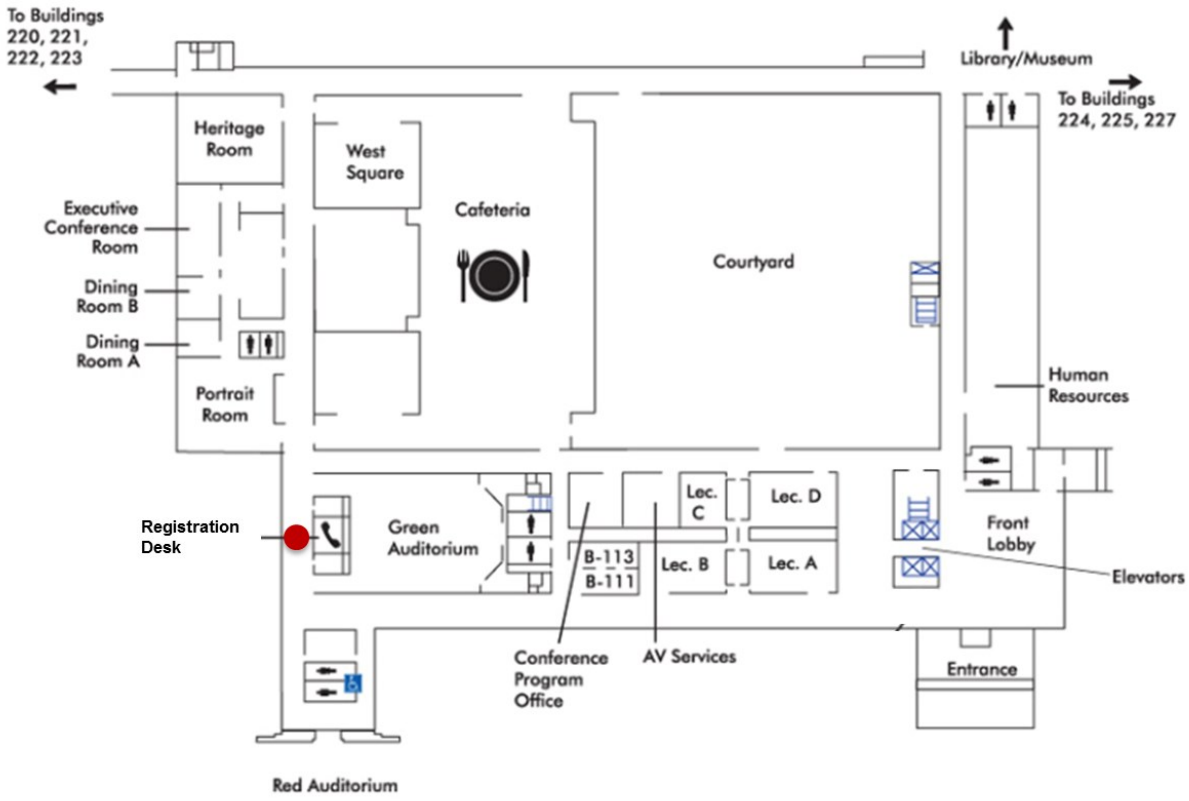
National Institute of Standards and Technology
U.S. Department of Commerce

Ask the Experts

If you have any questions for our panel members, please place in basket by registration desk or submit them to sec-forum@nist.gov by 11 am on 6/21/2017. This will allow our panel members to prepare a succinct answer.

Building 101 First Floor Map

Table of Contents



How to Access the NIST-Guest Wireless Network

NIST-Guest is broadcasted and is the network to connect your device with.

1. Connect wirelessly to SSID: **NIST-Guest**
2. Open your browser, as needed.
   - ◊ *If using iOS (iPhones and iPads), access a web page that does not use https:// (for example, http://www.apple.com) to get to the Access and Use Policy.*
   - ◊ *If using Android devices, a web page will automatically open with the Access and Use Policy.*
3. Review the complete Access and Use Policy by scrolling to the bottom of the Window. Acknowledge that you agree to the terms identified by selecting ACCEPT.

Device access will be blocked if (1) it is a NIST-owned device; (2) malware or other malicious activity is detected; or (3) inappropriate online behavior is detected.

Lunch—Cafeteria and Courtyard

Attendees may go through the regular NIST cafeteria line and pay on their own. Cash or credit is accepted. 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.

The main cafeteria is in the Administration Bldg. (Bldg. 101). Hours of operation:

- Breakfast: 7:30 am to 10:00 am
- Breakfast Break: 10:00 am to 11:00 am
- Lunch: 11 am to 2:00 pm
- Happy Hour: 2:00 pm to 3:00 pm (30 percent off on salad bar and hot bar)

The cafeteria promptly closes at 3:00 pm.

Going Off Campus

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.

Be sure to park in spaces with orange dot. These are reserved for visitors to NIST.

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

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

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

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

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

Tuesday, June 20, 2017

9:00 – 9:05 am	**Welcome** Charles H. Romine, Ph.D., Director, Information Technology Laboratory, (NIST); Victoria Yan Pillitteri, FCSM Co-Chairperson, Computer Security Division (NIST)	Dr. Romaine will provide welcoming introductions to NIST. Ms. Pillitteri will cover the agenda and logistics for the Offsite.
9:05 – 9:20 am	**Overview and Update: NIST Computer Security Division and Applied Cybersecurity Division** Matt Scholl, Computer Security Division Chief (NIST); Donna Dodson, Chief Cybersecurity Advisor, Information Technology Laboratory (NIST)	Mr. Scholl and Ms. Dodson will provide an update on the activities and publications of the Computer Security Division and Applied Cybersecurity Division.
9:20 – 9:55 am	**Update from the White House National Security Council** Heather King, Director for Cybersecurity Policy at the National Security Council Staff, Executive Office of the President	Ms. King will provide an overview of the national cybersecurity strategy and policy for the Trump Administration.
9:55 – 10:30 am	**Office of Management and Budget Update** Grant Schneider, Acting Federal Chief Information Security Officer, Office of Management and Budget (OMB)	Mr. Schneider will provide an overview and update of the Office of Management and Budget's cybersecurity strategy.
	10:30 – 10:45 am Break	
10:30 – 11:15 am	**FedRAMP Tailored** Matt Goodrich, FedRAMP Director, General Services Administration (GSA)	Mr. Goodrich will be presenting on the FedRAMP Tailored process for authorizing use of "Low-Impact Software-as-a-Service."
11:30 am – 12:15 pm	**Overview of the Software Quality Assurance Project and Software Assurance Marketplace** Kevin Greene, Software Assurance Program Manager, Department of Homeland Security (DHS)	Mr. Greene will provide an overview of the Software Quality Assurance project (SwQA) and the Software Assurance Marketplace (SWAMP). SwQA is developing innovative approaches to reduce the risk and cost of software failures by advancing research and development in new tool and techniques, and applying new and improved capabilities and vulnerability testing and evaluation.
	12:15 – 1:15 pm Lunch	
1:15 – 2:45 pm	**Applying the Cybersecurity Framework in Federal Agencies: Presentation and Panel Discussion** Matt Barrett, Cybersecurity Framework Program Manager, Applied Cybersecurity Division (NIST)	Mr. Barrett will provide an overview of Draft NISTIR 8170, The Cybersecurity Framework: Implementation Guidance for Federal Agencies, and moderate a panel discussion about Federal Cybersecurity Framework implementations. Panelists include: - Dom Cussatt, Acting CISO (VA) - Kelby Funn, Senior Information Security Specialist, Office of Information Technology/Security (SEC)
	2:45 – 3:00 pm Break (cafeteria closes at 3:00 pm)	

Tuesday, June 20, 2017 (cont.)

3:00 – 3:45 pm	**Top Down vs. Bottom Up Governance of Risk, What's Best?** Shahid Shah, Founder, NetSpective	Mr. Shah will be providing how an organization can move from continuous diagnostics and mitigation models to situational awareness approaches for cybersecurity governance seems to be a good direction for managing risk. Traditional "top-down" risk identification and governance is good for compliance but doesn't really do much to increase security; bottom-up approach to managing risk by letting system owners manage and own their risks is better but it's more time consuming.
3:45 – 4:30 pm	**Cybersecurity Dashboard on a Shoestring Budget** Kevin Colin, Criminal Investigations Cybersecurity Manager, Internal Revenue Service (IRS)	The Criminal Investigation's (CI) Cybersecurity Dashboard was developed to display the status of CI Cybersecurity FISMA reports, continuous monitoring, RBD, and POA&M efforts in one snapshot at the lowest cost possible. It was designed to educate and provide CI leadership, The CI Technical Operations Center, and Program/Project Managers a high-level view of their Cyber risk areas in one snapshot. It provide management with vectored, educated, mitigation decisions based on the dashboard snapshot before CDM was operational.
4:30 – 5:00 pm	**High Vulnerability Asset Overlay** John Simms, Continuous Diagnostics and Mitigation Program Manager, Department of Homeland Security	Providing adequate protection for America's High Value Assets (HVA) is critical to the economic and national security interests of the nation. DHS is developing an action plan and corresponding guidance to help federal agencies identify HVAs; select and implement appropriate safeguarding measures to protect HVAs, identify and implement monitoring processes, procedures, and technologies to detect compromises or losses to HVAs, identify and implement mechanisms to respond to compromises or losses of HVAs, and provide measures to recover from compromises or losses of HVAs.
	5:00 pm Closing Remarks	

Wednesday, June 21, 2017

9:00 – 9:25 am	**Welcome and Day 2 Overview** Jody Jacobs, FCSM Co-Chairperson, Computer Security Division (NIST)	Ms. Jacobs will give an overview of today's schedule.
9:25 – 10:45 am	**Pushing Computers to the Edge: Next Generation Security and Privacy Controls for Systems and IoT Devices** Ron Ross, NIST Fellow, Computer Security Division, Information Technology Laboratory	There is an urgent need to further strengthen the underlying systems, component products, and services that we depend on in every sector of the critical infrastructure—ensuring those systems, components, and services are sufficiently trustworthy and provide the necessary resilience to support the economic and national security interests of the United States. NIST Draft Special Publication 800-53 (Rev. 5) embarks on a proactive and systemic approach to develop and make available to a broad base of public and private sector organizations. Safeguard measures include security and privacy controls to protect the critical and essential operations and assets of organizations and the personal privacy of individuals.
	10:45 – 11:00 am Break	
11:00 – 11:45 am	**Infusing Cybersecurity into the Government Acquisition Process** Shon Lyublanovits, GSA/ITC IT Security Subcategory Manager/Director, Office of Security Services, General Services Administration (GSA)	Ms. Lyublanovits will discuss defining new ways of thinking when it comes to Cybersecurity and Security in Government acquisition.
11:45 am – 12:15 pm	**Government Accountability Office Update** Greg Wilshusen, Director of Information Security Issues, U.S. Government Accountability Office (GAO)	Mr. Wilshusen 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.
	12:15 – 1:15 pm Lunch	
1:15 – 2:15 pm	**"Ask the Experts" Panel** - Kelley Dempsey, Senior Information Security Specialist, Computer Security Division (NIST); - Rob Glenn, NIST Chief Information Security Officer and Office of Information Systems Management Information Technology Security and Networking Division Chief; - Beckie Koonge, Acting Chief Information Security Office (NOAA); - Kellie Riley, Chief Privacy Officer (OPM)	Do you have an information security implementation question that you've wanted a second (or third, or fourth) opinion on? This session will feature a panel of subject matter experts spanning a CISO, a member of the NIST FISMA team, an ISSM, and a Senior Accountable Officer for Privacy – ready to answer your questions. ***Please submit your questions for the experts via sec-forum@nist.gov or in the "Question Box" at the registration desk by 11 AM. Panelists will respond to submitted questions first before having an "Open Mic" session.***
	2:15 – 2:30 pm Break (cafeteria closes at 3:00 pm)	
2:30 – 3:00 pm	**NISTIR 8011—Automation Support for Security Control Assessments** Kelley Dempsey, Senior Information Security Specialist, Computer Security Division (NIST)	Ms. Dempsey will be presenting on recently released NIST IR 8011, Automation Support for Security Control Assessments.
3:00 – 5:00 pm	*[Optional]* **Applying the Cybersecurity Framework in Federal Agencies Working Session**	Hosted by Matt Barrett (NIST) in the NIST West Square or Green Auditorium.

Matt Barrett—Matt Barrett and his team are responsible for establishing and maintaining relationships with both private and public sector Cybersecurity Framework stakeholders. Mr. Barrett is known for his leadership of NIST's Security Content Automation Protocol program and the Office and Management and Budget's Federal Desktop Core Configuration initiative (predecessor to US Government Consensus Baseline).

Kevin Colin—Kevin Colin currently serves as Manager, Criminal Investigation (CI) – Cybersecurity, for the internal Revenue Service (IRS). He is responsible for leading and managing a 9-member team that ensures CI's compiles with Cybersecurity guidance, as well as provide security continuous monitoring of the CI networks to protect the Confidentiality, Integrity, and Availability (CIA) of its data and information. Prior to serving at the IRS, Kevin also served for 3 years as a Research and Development (R&D) Computer Network Defense Analyst for the Johns Hopkins Applied Physic Laboratory (JHU/APL). Kevin also served as a team lead with the coveted National Security Agency "Blue Team", and retired as a Major in the United States Air Force after serving 27 years.

Kelley Dempsey—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 On-going 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.

Donna Dodson—Donna Dodson is the Associate Director and the Chief Cybersecurity Advisor for the National Institute of Standards and Technology (NIST). She is also the Director of NIST's National Cybersecurity Center of Excellence (NCCoE). Ms. Dodson oversees ITL's cyber security program to conduct research, development and outreach necessary to provide standards, guidelines, tools, metrics and practices to protect the information and communication infrastructure. Under her leadership, ITL collaborations with industry, academia and other government agencies in research areas such as security management and assurance, cryptography and systems security, identity management, security automation, secure system and component configuration, test validation and measurement of security properties of products and systems, security awareness and outreach and emerging security technologies. In addition, Donna guides ITL programs to support both national and international security standards activities. She recently led the establishment of the NIST NCCoE. Donna received two Department of Commerce Gold Medals and three NIST Bronze Medals.

Kelby Funn—Kelby Funn has been at the U.S. Securities and Exchange Commission six years, supporting the CISO currently in the Privacy and Information Assurance Branch. During his tenure, he has supported information security through the life cycle, performing annual internal control reviews in support of OMB Circular A-123, supporting the annual management assurance statement of the Office of Information Technology and assembling external reporting metrics and documentation pertaining to the information security program to the White House and Congress. Kelby's career included supporting CISOs and IGs in their annual reporting requirements to the White House and Congress. He's been around since the GISRA (Government Information Security Act) days.

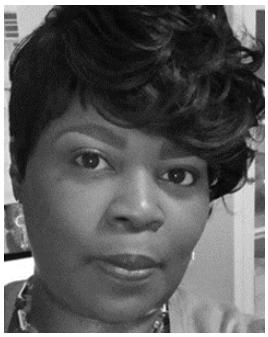
Rob Glenn—Rob Glenn is the NIST Chief Information Security Officer and the Office of Information Systems Management (OISM) Information Technology Security and Networking Division Chief. Mr. Glenn is responsible for directing NIST's operational cybersecurity program, including the management of many of NIST's cybersecurity systems and services protecting NIST's information and information systems. Mr. Glenn is also responsible for the management of NIST's wired and wireless network services supporting Gaithersburg, MD and Boulder, CO campuses. Mr. Glenn joined NIST in 1987 and spent 13 years in the NIST Information Technology Laboratory Advanced Network Technologies Division where he led and supported network and network security standards efforts. During this time he developed protocol prototypes and testing tools while working closely with other government agencies and industry supporting interoperability testing and co-authoring Internet standards.

Matt Goodrich—Matt Goodrich is the Director for the Federal Risk and Authorization Management Program (FedRAMP) in GSA's Office of Citizen Services and Innovative Technologies. 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. Matt has focused his career on removing the barriers to cloud adoption across the Federal government. Matt has authored and co-authored multiple integral federal documents.

Kevin Greene—Kevin Greene is a program manager in the Cyber Security Division for the Homeland Security Advanced Research Projects Agency (HSARPA) at DHS S&T. Mr. Greene is responsible for the Software Quality Assurance and Software Assurance Marketplace projects, which includes creating improvements for testing, analysis and evaluation techniques used in software quality assurance tools.

Heather King—Heather King is the Director for Cybersecurity Policy at the National Security Council Staff, Executive Office of the President.

Beckie Koonge—Beckie Koonge manages and oversees the National Weather Service's compliance with the Federal Information Security Management Act (FISMA) and implementation of IT security best practices. She and her team manage NWS-wide cybersecurity initiatives, programs, and monitoring which includes the Compliance and Assessment services for the systems owned and operated by NWS. Prior to joining NWS, she was a senior lead Information Security Analysis for Treasury's Office of Fiscal Service. Ms. Koonge has extensive experience in policy development and implementation, compliance, FISMA oversite, and coordinating and conducting assessments of a wide variety of IT systems across the federal government from critical financial systems processing trillions of dollars, to systems that provide time sensitive forecasts, alerts, or warnings of impending weather events. She currently advises the senior management officials at NOAA and NWS on POA&M management, key security metrics, system assessment status, system risk, and strategic direction for future program improvements. She is a change agent with a focus to improve cybersecurity and risk management within her agency.



Shon Lyublanovits—Shon Lyublanovits is the IT Security Category Manager and Director of the Security Services Division for the Office of Integrated Technology Services (ITS) in GSA's Federal Acquisition Service (FAS). The Federal Acquisition Service provides buying platforms and acquisition services to Federal, State and Local governments for a broad range of items from office supplies to motor vehicles to information technology and telecommunications products and services. As an organization within FAS, ITS provides access to a wide range of commercial and custom IT products, services and solutions.

Kellie Riley—Kellie Riley joined OPM in October of 2016 as Chief Privacy Officer. She serves as the principal privacy advisor to the OPM Director and is responsible for formulating and implementing OPM policies related to the collection, maintenance, and use of personally identifiable information. Her responsibilities include ensuring compliance with the Privacy Act, the privacy provisions of the E-Government Act, and other privacy-related laws, regulations, and guidance throughout OPM. Prior to joining OPM, Ms. Riley spent five years at the Department of Homeland Security. As an Attorney Advisor in the Legal Counsel Division of the Office of the General Counsel, she provided legal advice regarding the Privacy Act, E-Government Act, and other privacy-related legal issues to the DHS Privacy Office. She later served as a Senior Director in the DHS Privacy Office where she was responsible for privacy policy development and implementation, breach response, and information sharing. Ms. Riley began her government service with the Federal Trade Commission as an attorney in the Bureau of Consumer Protection. There she developed expertise in such privacy-related issues as the Gramm-Leach-Bliley Financial Privacy Rule, the Fair Credit Reporting Act, and the FTC Act. In addition, she was an Attorney-Advisor to Commissioner Mozelle Thompson advising on a variety of international and domestic consumer protection issues.

Charles Romine—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.

Ron Ross—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.

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

Matthew Scholl—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.

Shahid Shah is an award-winning Government 2.0, Health IT, and Medical Device Integration software expert and internationally-recognized thought leader with over 27 years of technology strategy, software engineering, entrepreneurship, speaking, and writing experience. He's a serial entrepreneur that has co-founded and led Netspective.com, Physia.com, InfluentialNetworks.com, HealthcareGuy.com, HITSphere.com, and simplifyMD.com within the last few years; he has another two stealth startups in the works. His primary responsibility is as CEO of Netspective Communications, a computer software architecture & engineering firm delivering custom software for in-house, outsourced, or offshore solutions. Shahid also serves as a senior technology advisor to OMB's Budget System Branch, the eGov Budget Formulation & Execution Line of Business (BFELoB.gov), Veterans Affairs (VA.gov), OSEHRA.org, and Millenni-um Challenge Corporation (MCC.gov).

John Simms—John Simms currently serves as the Program Manager for the Department of Homeland Security's Continuous Diagnostics and Mitigation (CDM) Program. Prior to joining the Department of Homeland Security, John served as the Chief Information Security Officer (CISO) at the U.S. Food and Drug Administration (FDA), and a Senior Advisor to the CISO at the U.S. Department of State.

Gregory Wilshusen—Gregory Wilshusen is Director of Information Security Issues at Government Accountability Office (GAO), where he leads information security-related studies and audits of the federal government. He has over 35 years of auditing, financial management, and information systems experience.

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
Peggy Himes, Jody Jacobs, and Victoria Yan Pillitteri

Thank you…..

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

◊ FCSM Working Group 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)
- Peggy Himes, FCSM Conference Administrator
- Patrick O'Reilly and Nikki Keller for website maintenance

◊ NIST Public Affairs Office
- Mary Lou Norris, NIST Conference Office Director
- Crissy Robinson, NIST Conference Administrator
- Karen Startsman, registration and logistics
- NIST AV Technicians

◊ Conference presentations will be posted after the conference to the FCSM Website http://csrc.nist.gov/groups/SMA/forum/ (soon to be https://beta.csrc.nist.gov/Projects/Forum)

Next FCSM Bi-Monthly Meeting will be August 16, 2017 at the NIST Gaithersburg, MD Campus in the NIST Heritage Room.

Participation in the Forum list serve is limited to U.S. federal and state government employees only who participate in the management of their organization's computer security program and have a .gov, .mil, or state government email address. However, exceptions for contractors serving in higher positions such as ISSOs or CISOs have been made as long as they have a government-sponsored email address.
To request to join, email: sec-forum@nist.gov

Notes: