Federal Computer Security Managers’ Forum Annual Offsite

Program and Speaker Profiles

NIST Green Auditorium

May 8-9, 2019

National Institute of Standards and Technology
U.S. Department of Commerce
Accessing NIST-Guest Wireless Network

- The guest wireless network is NIST-Guest
- To connect from a mobile device, open your browser
  - If using iOS (iPhones and iPads), access a web page that does not use https:// (for example, 1.1.1.1) to get to the Access and Use Policy.
  - If using Android devices, a web page will automatically open with the Access and Use Policy.
- 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.

Cafeteria Hours

- Attendees may go through the regular NIST cafeteria line and pay on their own. Cash or credit is accepted. You can order sandwiches from the grill or select from the hot and salad bar. Sandwiches from the grill are priced separately. The hot and salad bar 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: 11:00 am to 2:00 pm
  - Happy Hour: 2:00 pm to 3:00 pm (30% off on salad bar and hot bar)
- The cafeteria promptly closes at 3:00 pm.

Going Off Campus and Parking

- Attendees can go off campus 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.
- Please park in the Building 101 parking lot in spaces with yellow dots. These are reserved for NIST visitors.
Please Remember....

- Mute your cellphones once the Forum begins.
- Hold questions until the Q&A period for each session. Microphones are located at each side of the auditorium.
- Only Ron Ross’ presentation will be recorded; Q&A will not be recorded.
- Keep all issues and questions discussed at the forum confidential.
- Take all personal belongings with you at the end of each conference day. NIST is not responsible for lost or stolen items.
- Continuing Education forms are available online; a limited number of Continuing Education forms are available at the registration desk. Attendees are responsible for submitting to your certifying authority.
- NIST Conference Services will email attendees an evaluation following the event, we appreciate you taking the time to complete and provide feedback.
- Presentations (with permission) will be posted to the Forum Website 7-10 days following the conference.
- Email sec-forum@nist.gov with any questions during or after the conference.
### Wednesday, May 8, 2019

<table>
<thead>
<tr>
<th>Time</th>
<th>Session</th>
</tr>
</thead>
<tbody>
<tr>
<td>9:00 – 9:05 am</td>
<td><strong>Forum Welcome and Day 1 Overview</strong></td>
</tr>
<tr>
<td></td>
<td>Jody Jacobs, Forum Chairperson, Computer Security Division, NIST</td>
</tr>
<tr>
<td></td>
<td>Ms. Jacobs will cover the agenda and logistics for the meeting.</td>
</tr>
<tr>
<td>9:05 – 9:15 am</td>
<td><strong>Welcome to NIST and Event Overview</strong></td>
</tr>
<tr>
<td></td>
<td>James St. Pierre, Deputy Director, Information Technology Laboratory, NIST</td>
</tr>
<tr>
<td></td>
<td>Mr. St. Pierre will provide welcoming introductions to NIST.</td>
</tr>
<tr>
<td>9:15 – 9:45 am</td>
<td><strong>The Federal Acquisition Supply Chain Security Act of 2018—the Law and its Implementation</strong></td>
</tr>
<tr>
<td></td>
<td>Michael Halas, Director for Government Cybersecurity, National Security Council (NSC)</td>
</tr>
<tr>
<td></td>
<td>The President signed the Federal Acquisition Supply Chain Security Act of 2018 into law in late December 2018, as part of the Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure Technology Act (SECURE) Technology Act. This new law creates a unified, whole-of-government approach to protecting federal systems from supply chain risks. In particular, it establishes the Federal Acquisition Security Council and empowers it to take various actions to protect the Nation from supply chain risks, including (1) identifying standards and guidelines that executive branch agencies must use to manage their supply chain risk; (2) identifying a federal agency to act as a supply chain risk information clearing house to facilitate the sharing of supply chain information inside and outside of the government; and (3) identifying federal agencies to provide shared supply chain risk management services and solutions to other federal agencies. The law also authorizes the Department of Homeland Security, the Department of Defense, and the Office of the Director of National Intelligence to issue &quot;removal and exclusion orders&quot; with appropriate legal protections to protect federal systems from supply chain risks within their respective areas of authority. Mr. Halas will discuss this law and its implementation.</td>
</tr>
<tr>
<td>9:45 – 10:25 am</td>
<td><strong>National Risk Management Center’s Information and Communications Technology (ICT) Supply Chain Risk Management Task (SCRM) Force Update</strong></td>
</tr>
<tr>
<td></td>
<td>Mark Kneidinger, Deputy Director, National Risk Management Center, Department of Homeland Security (DHS)</td>
</tr>
<tr>
<td></td>
<td>Mr. Kneidinger will brief participants on the highlights of the National Risk Management Center (NRMC) Information and Communications Technology (ICT) Supply Chain Risk Management (SCRM) Task Force activity. The ICT SCRM is one of several key initiatives of the NRMC. The ICT SCRM task force includes 20 industry members each from the IT Sector, Communications sector and the interagency. The Task Force recently launched four main work streams with a range of focus, from establishing criteria for threat-based evaluation to criteria for Qualified Bidder and Manufacturer List(s). The task force also intends to be one of the primary touch points between government and industry for the newly created Federal Acquisition Security Council.</td>
</tr>
<tr>
<td>10:25 – 10:45 am</td>
<td><strong>Break</strong></td>
</tr>
<tr>
<td>10:45 – 11:25 am</td>
<td><strong>Update from the Office of Management and Budget</strong></td>
</tr>
<tr>
<td></td>
<td>Taylor C. Roberts, Cybersecurity Advisor, Cyber and National Security Unit, Office of the Federal Chief Information Officer, Office of Management and Budget (OMB)</td>
</tr>
<tr>
<td></td>
<td>Mr. Roberts will provide an update on the work the Office of the Federal Chief Information Officer is doing in relation to the President’s Management Agenda.</td>
</tr>
<tr>
<td>11:25 am – 12:05 pm</td>
<td><strong>Cybersecurity Performance Insights and Data Analytics</strong></td>
</tr>
<tr>
<td></td>
<td>Frank Husson, Cybersecurity Performance Management Branch Chief, Federal Network Resilience, Cybersecurity Division, Cybersecurity and Infrastructure Security Agency, Department of Homeland Security (DHS)</td>
</tr>
<tr>
<td></td>
<td>Jennifer Oar, Cybersecurity Performance Management Business Intelligence &amp; Advanced Data Analytics Section Chief, Federal Network Resilience, Cybersecurity Division, Cybersecurity and Infrastructure Security Agency, Department of Homeland Security (DHS)</td>
</tr>
<tr>
<td></td>
<td>Mr. Husson and Ms. Oar will provide an overview of cybersecurity performance metrics trends and opportunities to improve federal network resilience, including Fiscal Year 18 Federal Information Security Modernization Act (FISMA) metrics data visualizations.</td>
</tr>
</tbody>
</table>
### Small Agency Organization

**12:05 - 12:40 pm**

*Alen Kirkorian, Division Chief, Innovative Strategy and Security Office of the Chief Architect, Department of State (DOS)*

*Dan Jacobs, Office of Information, Integrity, Access Cybersecurity Program Coordinator, General Services Administration (GSA)*

The Small and Micro Agency CISO Council (SMAC) is an informal gathering of cybersecurity professionals designed to share information, coordinate activities, demonstrate new/emerging technologies, and influence government-wide decision making on cyber matters. Mr. Kirkorian and Mr. Jacobs will discuss how the SMAC operates, and how they can help other small federal agencies.

### Lunch

**12:40 – 1:40 pm**

### Update from the U.S. Government Accountability Office

**1:40 – 2:20 pm**

*Nick Marinos, Director, Cybersecurity and Information Management Issues, Government Accountability Office (GAO)*

*Vijay D’Souza, Director, Information Technology and Cybersecurity Issues, GAO*

Mr. Marinos and Mr. D’Souza will provide an update on the activities and publications of the Government Accountability Office (GAO). This presentation will address key issues related to information security and cybersecurity and highlight current GAO key initiatives.

### Security Control Overlay Development

**2:20 – 3:00 pm**

*Tameika Turner, Risk Management Program, Branch Chief, Office of Information Security, Census Bureau*

*Ayokunmi Akingbade, Information Technology Specialist, Office of Information Security, Census Bureau*

As organizations work to implement new technologies and comply with evolving cyber mandates, federal agencies must have agile cyber programs that simultaneously support mission success and protect the confidentiality, integrity, and availability of their information and information systems. Cyber programs can make their processes more dynamic and scalable by using security control overlays, which facilitate a more tailored efficient approach to compliance. Security control overlays complement security control baselines by allowing for the addition or elimination of controls against organizational requirements. The Census Bureau has developed and implemented a methodology that establishes and applies security control overlays to an information system’s security control baseline (e.g., common control provider application, FedRAMP packages, policy requirements) based on an information system’s business and technical requirements. Ms. Turner and Mr. Akingbade will present on this approach that can benefit organizations by reducing subjectivity and promoting consistency during system categorization and control selection.

### User Context in Phishing Susceptibility and Implications for Practitioners

**3:00 – 3:40 pm**

*Kristen Greene, Cognitive Scientist, Information Access Division, NIST*

As phishing continues to evolve, what is your organization doing to stay off the hook? Based on 4.5 years of NIST phishing exercise data, Ms. Greene will present operational take-aways for security practitioners.

### Federal Information Processing Standard (FIPS) 140-3 Encryption

**3:40 – 4:15 pm**

*Michael Cooper, Security Test, Validation and Measurement Group Manager, Computer Security Division, NIST*

Mr. Cooper will provide an update on the Federal Information Processing Standard (FIPS) 140-3 Encryption, designed to coordinate the requirements and standards for cryptography modules that include hardware and software with government and industry to establish more secure systems and networks by developing, managing and promoting security assessment tools, techniques, services, and supporting programs for testing, evaluation, and validation.
<table>
<thead>
<tr>
<th>Time</th>
<th>Session</th>
</tr>
</thead>
<tbody>
<tr>
<td>9:00 – 9:05 am</td>
<td>Forum Welcome and Day 2 Overview</td>
</tr>
<tr>
<td>Jody Jacobs, Forum Chairperson, Computer Security Division, NIST</td>
<td>Ms. Jacobs will give an overview of today’s meeting.</td>
</tr>
<tr>
<td>9:05 – 9:20 am</td>
<td>Overview and Update: NIST Computer Security Division and Applied Cybersecurity Division</td>
</tr>
<tr>
<td>Matt Scholl, Computer Security Division (CSD) Chief, NIST</td>
<td></td>
</tr>
<tr>
<td>Kevin Stine, Applied Cybersecurity Division (ACD) Chief, NIST</td>
<td>Mr. Scholl and Mr. Stine will provide an update on the activities and publications of the CSD and ACD.</td>
</tr>
<tr>
<td>9:20 – 10:20 am</td>
<td>Next Generation Cybersecurity and Risk Management Guidance—2019 and Beyond</td>
</tr>
<tr>
<td>Ron Ross, NIST Fellow, Computer Security Division, NIST</td>
<td>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.</td>
</tr>
<tr>
<td>10:20 – 10:40 am</td>
<td>Break</td>
</tr>
<tr>
<td>10:40 – 11:30 am</td>
<td>NIST Privacy Framework</td>
</tr>
<tr>
<td>Naomi Lefkovitz, Senior Privacy Policy Advisor, Applied Cybersecurity Division, NIST</td>
<td>Ms. Lefkovitz and Ms. Nadeau will provide an update on the NIST Privacy Framework developed in collaboration with private and public sector stakeholders, to help organizations: better identify, assess, manage, and communicate privacy risks; foster the development of innovative approaches to protecting individuals’ privacy; and increase trust in products and services.</td>
</tr>
<tr>
<td>Ellen Nadeau, Privacy Risk Strategist, Applied Cybersecurity Division, NIST</td>
<td></td>
</tr>
<tr>
<td>11:30 – 11:55 am</td>
<td>NIST Privacy Engineering Collaboration Space</td>
</tr>
<tr>
<td>Kaitlin Boeckl, Privacy Risk Strategist, Applied Cybersecurity Division, NIST</td>
<td>Explore NIST’s recently-launched Privacy Engineering Collaboration Space: an online venue open to the public where practitioners can discover, share, discuss, and improve upon open source tools, solutions, and processes that support privacy engineering and risk management. The space has launched with an initial focus on de-identification, to include differential privacy techniques, and privacy risk assessment. Ms. Boeckl will provide a demo of the space, get an overview of contributions to date, and learn how to contribute.</td>
</tr>
<tr>
<td>11:55 am – 12:35 pm</td>
<td>PBGC’s Government to Government Shared Services Authorization to Use (ATU) Guidance</td>
</tr>
<tr>
<td>Susan Schultz-Searcy, Security and Privacy Assessment and Authorization Program Lead, Enterprise Cybersecurity Division, Pension Benefit Guaranty Corporation (PBGC)</td>
<td>The drive for more agencies to use federal Information Technology shared services from Office of Management and Budget’s (OMB’s) Cloud First initiative to data center consolidations has left these agencies with a new challenge in managing risk in systems, services, and applications operated outside the bounds of their system inventories. Over the last two years, OMB and NIST have to carve out new authorization options for agencies to grant when using these systems, services or applications. PBGC published Authorization to Use (ATU) Guidance based on the Risk Management Framework to assist the agency in managing the security and privacy risks of using IT shared services offered by other federal agencies. PBGC has granted an ATU and expects to see additional ATUs for shared services within the financial and HR spaces later this year. Ms. Schultz-Searcy will share PBGC’s experience crafting the ATU approach based on federal guidance and feedback from the PBGC Cybersecurity and Privacy Council and plans to move forward with the new authorization option.</td>
</tr>
<tr>
<td>12:35 – 1:15 pm</td>
<td>Open, Public, Electronic, and Necessary (OPEN) Government Data Act</td>
</tr>
<tr>
<td>Maya Bernstein, Senior Advisor, Privacy Policy, Health and Human Services (HHS)</td>
<td>Ms. Bernstein will discuss the Open, Public, Electronic, and Necessary (OPEN) Government Data Act, passed in January 2019 which mandates federal agencies to publish all their information as open data - using standardized, non-proprietary formats.</td>
</tr>
</tbody>
</table>
Michael Halas is the Director for Government Cybersecurity on the staff of the National Security Council (NSC). In that role, he coordinates cybersecurity policy efforts across the federal government and oversees cybersecurity activities related to government systems. At NSC, he played key roles in leading the development and rollout of the National Cyber Strategy and in the creation of the Federal Acquisition Supply Chain Security Act of 2018. In his previous position, as an attorney-advisor focusing on cybersecurity in the Office of the General Counsel of the U.S. Department of Homeland Security (DHS), he provided legal counsel on a wide range of cybersecurity-related activities, including incident response, risk assessments, information sharing, and federal cybersecurity. He also negotiated technology agreements, advocated the DHS’s positions, and reviewed and drafted legislation. Mike also spent time at DHS as an attorney-advisor in DHS’s Honors Attorney Program, where he rotated through the legal offices of the Secret Service, DHS headquarters, the Federal Emergency Management Agency, and Customs and Border Protection. Before joining DHS, Mike was a judicial law clerk for United States District Judge Eric N. Vitaliano of the Eastern District of New York, a judicial law clerk for Justice Carolyn Berger of the Delaware Supreme Court, a patent agent and technology specialist at WilmerHale LLC, and an engineer at IBM. He holds a J.D. from the Fordham University School of Law and a B.S. in electrical and computer engineering from the Rutgers University School of Engineering and is a Certified Information Systems Security Professional.

James St. Pierre is Deputy Director of the Information Technology Laboratory (ITL). ITL is one of six research laboratories within the National Institute of Standards and Technology (NIST) with an annual budget of $120 million, more than 350 employees, and about 160 guest researchers from industry, universities, and foreign laboratories. Mr. St. Pierre oversees a research program designed to promote U.S. innovation and industrial competitiveness by developing and disseminating standards, measurements, and testing for interoperability, security, usability, and reliability of information systems, including cybersecurity standards and guidelines for federal agencies and U.S. industry. In addition, Mr. St. Pierre oversees ITL’s Internet of Things (IoT) and Big Data research programs.

Mark Kneidinger is the Deputy Director of the DHS National Risk Management Center (NRMC), within the Cybersecurity and Infrastructure Security Agency (CISA). The NRMC is an organization working in collaboration with the industry that generates solutions to reduce cyber and physical strategic risk to the Nation’s critical infrastructure. Prior to this role, Mr. Kneidinger had been the Director of the Federal Network Resilience (FNR) Division, within CISA’s Office of Cybersecurity and Communication (CS&C). In this position, Mr. Kneidinger led FNR’s activity in representing and supporting implementation of CS&C Cyber Programs to all Executive Branch Departments & Agencies in collaboration with OMB, NSC, the CIO Council and the individual agency CIOs and CISOs. Prior to joining DHS, Mr. Kneidinger held IT Executive leadership positions in the commercial sector for Fortune 500 Corporations, including roles as CTO, Vice President and Managing Partner. Mr. Kneidinger has further held Chief Information Office (CIO) positions in New York and Virginia as well as served as a White House appointee in the position of Deputy Assistant Administrator and CIO for the U.S. Agency for International Development (USAID).
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.

Frank Husson is a senior cybersecurity program manager at the Department of Homeland Security, with over 30 years of progressive experience in both the public and private sectors. His experience includes Program and Portfolio Management (PPM), Cyber Security, Policy Development, Incident Management, Architecture and Modeling, and Performance Monitoring. Since joining DHS in 2016, Frank has led DHS efforts to measure and monitor cybersecurity performance through development and enhancement of FISMA metrics and CyberStat program reviews. Prior to joining DHS, Frank established and managed an enterprise-wide Project Management Office, as well as developed and implemented operational cybersecurity programs at multiple federal agencies.

Jennifer Oar has worked in the homeland security field for 14 years, leading data and innovation teams for the past 5 years. In 2016, Jennifer joined FNR to stand up their cybersecurity performance management data analytics team and accelerate analytic product delivery. Previously she worked in the DHS Office of Intelligence and Analysis (I&A) leading the Analytic Innovation Cell to address counterterrorism, border security, and cybersecurity analytic challenges. In 2015, Jennifer was awarded the Secretary’s Meritorious Service Award for collaboration, innovation, and outstanding service in creating solutions to help improve the Department’s analytic capabilities. Jennifer earned a Master in Public Administration (MPA) from The American University, and is an Adjunct Instructor for Medaille College’s Homeland Security Program.
Alen Kirkorian joined the Department of State in September 2014, as the lead of the Innovation, Strategy, and Security branch of the Office of the Chief Architect (OCA). His core focus is implementing innovative solutions for diplomacy with a diverse team of business and technical subject matter experts. He has over 27 years of experience with Information Technology and Security from a wide variety of industries. At the Overseas Private Investment Corporation (OPIC) he was the Chief Information Security Officer, while at the Agency for International Development (USAID), he held IT Program Management roles and managed several large worldwide programs and projects leading Information Technology, Technology Operations, and Security Operations teams. Prior to those roles, Alen served as Program Manager for Cachendo, Technical Program Manager for True North Solutions and for Morgan Stanley in New York, New York, as well as a Senior Security Architect for a number of financial and health firms in the New York City area. He earned a Bachelor of Science degree from Manhattan College and a Master's in Computer Science from Steven's Institute of Technology.

Dan Jacobs serves as the Office of Information, Integrity, and Access Cybersecurity Program Coordinator within the Office of Government-wide Policy of the U.S. General Services Administration. Mr. Jacobs has 20+ years of IT positions with several major corporations including Computer Sciences Corporation, CACI, Northrop Grumman, and the Japanese telecom KDD. As a government civilian, Mr. Jacobs has served in roles as varied as directing IT and telephony services for a large, multi-mission installation to enterprise network security for the Army's European Theater to Computer Network Operations and intelligence fusion.

Nick Marinos joined the U.S. Government Accountability Office (GAO) in 2002 and serves as a Director within GAO’s Information Technology and Cybersecurity team. He manages audit teams that perform government wide and agency-specific reviews in the areas of cybersecurity, critical infrastructure, privacy, and data protection across all major federal agencies. Nick holds a Master’s in Business Administration and a Bachelor of Science degree from Virginia Tech. He also serves as a member of Virginia Tech’s advisory boards for their MBA program and Business Information Technology department.
Vijay D’Souza leads multiple efforts to evaluate the performance of federal programs in the areas of cybersecurity and information technology. He leads GAO’s eSecurity Lab, which provides technical support to GAO’s cybersecurity engagements. Previously Vijay led GAO’s efforts to enhance its data analytics capabilities. He has also led audits in areas such as improper payments and IT program management. Vijay has been at GAO since 2001. He has an M.B.A from the University of California Berkeley and a B.S. in Engineering from the University of Maryland, College Park.

Tameika Turner started working at the Census Bureau in 2006 in the Mixed Tour Program as an Office Automation Clerk for the Office of the Chief Information Officer. She was then transferred to the Office of Information Security in 2008 as a Computer Assistant for the Security Reviews and Policy Staff. Ms. Turner was promoted to the position of IT Specialist in the Certification and Accreditation Branch in 2011. She was instrumental in the Census Bureau’s transition from the 3-year Certification & Accreditation (C&A) cycle to the Risk Management Framework (RMF) through: the development of IT system risk profiles driven by a quantitative risk scoring methodology, the establishment of enterprise common controls, and the deployment of a Governance, Risk, and Compliance repository. She also leads and coordinates data calls for auditors and other external entities. In her new role as the Risk Management Program Branch Chief, Ms. Turner oversees security policy & procedure development, leads the coordination of data calls from external auditors, and continues to support the Assessment & Authorization (A&A) activities leading up to the 2020 Decennial Census. Ms. Turner graduated from Bowie State University with a B.A. in Business Administration and is working toward a master's degree in Information Assurance. She was awarded the Department of Commerce Gold Medal Award in 2014 and has obtained the ISC2 Certified Authorization Professional (CAP) certification.

Kunmi Akingbade is a Senior Manager at Deloitte in the Cyber practice. He specializes in the following areas: helping federal agencies establish a comprehensive risk management program by developing security strategies & policies, managing the deployment/integration of Governance, Risk, and Compliance (GRC) tools, preparing/executing security audit readiness activities, and conducting security assessments. Mr. Akingbade currently holds the following industry certifications: Certified Information Systems Security Professional (CISSP), Certified Information Systems Auditor (CISA), and Certified Information Privacy Professional (CIPP/G). He graduated from the University of Maryland, College Park with a degree in Information Systems and Operations Management, and a certificate in entrepreneurship. He continued his education at the University of Maryland, University College obtaining dual Master’s degrees in Cybersecurity and Business Administration.
Kristen Greene is a Cognitive Scientist at NIST, the National Institute of Standards and Technology. She conducts usability and human factors research for NIST’s PSCR (Public Safety Communications Research) and usable cybersecurity programs. She has an M.A. and Ph.D. in Cognitive Psychology from Rice University. She is an experienced researcher, having conducted research in the Attention and Perception Laboratory at the University of South Carolina, the Usability Testing and Analysis Facility at NASA Johnson Space Center, the Computer Human Interaction Laboratory at Rice University, and now the Information Technology Laboratory at NIST.

Michelle Steves is an Information Systems Analyst at NIST, the National Institute of Standards and Technology. She conducts usability and human factors research for NIST’s PSCR (Public Safety Communications Research) and usable cybersecurity programs. She has a B.A. in Mathematics and Computer Science from Western Maryland College. She is an experienced researcher, having conducted research in the Information Technology and Manufacturing Technology Laboratories at NIST.

Mary Theofanos is a Computer Scientist with the National Institute of Standards and Technology where she performs research on usability and human factors of systems. Mary is the principal architect of the Usability and Security Program evaluating the human factors and usability of cyber security and biometric systems.

Michael Cooper is the manager of the Security Testing, Validation, and Measurement Group within the Computer Security Division at NIST. Mr. Cooper brings over 30 years of technical and management experience to this role based on previous positions held in the military, government service, and consulting. His technical background consisted primarily of system engineering and database administration. Michael holds a Bachelor of Science in Computer Science from the University of Maryland.
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) 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.

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 (FISMA) 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.
**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. She leads the privacy engineering program, which focuses on developing privacy risk management processes and integrating solutions for protecting individuals’ privacy into information technologies, including digital identity services, IoT, smart cities, big data, mobile, and artificial intelligence. She also leads the development team for the NIST Privacy Framework.

Before joining NIST, she was the Director for Privacy and Civil Liberties in the Cybersecurity Directorate of the National Security Council in the Executive Office of the President. Her portfolio included the National Strategy for Trusted Identities in Cyberspace as well as addressing the privacy and civil liberties impact of the Obama Administration’s cybersecurity initiatives and programs.

Prior to her tenure in the Obama Administration, 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 School of Law.

---

**Ellen Nadeau** is part of the Privacy Engineering Program at the National Institute of Standards and Technology (NIST), where she works to develop and pilot privacy risk management guidance and tools for organizations across sectors. She specializes in privacy-enhancing identity management solutions. 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. 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.

---

**Kaitlin Boeckl** is a privacy risk strategist at the National Institute of Standards and Technology (NIST) as part of the Privacy Engineering Program and the Privacy Framework team. Katie manages the Privacy Engineering Collaboration Space, works to advance international privacy standards, and develops privacy risk management guidance. At NIST, she has served as a co-author for NIST Special Publication 800-37, revision 2: Guide for Applying the Risk Management Framework to Federal Information Systems, worked to implement the National Strategy for Trusted Identities in Cyberspace (NSTIC), and contributed to Special Publication 800-63, revision 3: Digital Identity Guidelines. Katie has a B.A. in English from the University of Maryland, College Park, where she specialized in technology through a digital cultures honors program.
Susan Schultz-Searcy is the Security and Privacy Assessment & Authorization Program Lead for the Enterprise Cybersecurity Division with Pension Benefit Guaranty Corporation. In her role, she manages the A&A process for PBGC information systems, and is responsible for the Risk Management Process, and several other cybersecurity compliance and oversight activities. She has also served on interagency working groups including the DHS Ongoing Authorization Working Group. Prior to her role at PBGC, Mrs. Schultz Searcy served as an IT Specialist for Compliance and Oversight and IT Audit liaison in the Office of Cybersecurity within the Office of Chief Information Officer at the U.S. Department of Commerce. Mrs. Schultz Searcy began her federal cybersecurity career in February 2011. Prior to her public service, she served in the private sector beginning in June 2009 performing compliance reviews and assessments supporting federal clients. Mrs. Schultz Searcy holds a CISA certification and was a member of the CXO Fellows Class of 2016-2017.

Maya Bernstein is the lead career civil servant responsible for privacy policy in the Office of the Secretary. Ms. Bernstein's portfolio comprises a wide variety of subjects involving personally-identifiable information including medical records privacy, electronic health records, health information technology, consumer-generated health information, genetic discrimination, family and child welfare, drug abuse and mental health records, prescription drug surveillance, research, statistical confidentiality, personal records, anti-terrorism and counterintelligence, and incident response. Ms. Bernstein serves as lead staff to an advisory committee to the Secretary of Health & Human Services and regularly represents HHS on government-wide policy development teams, including White House task forces and public-private partnerships.

To our distinguished speakers,

When planning an event such as the Federal Computer Security Managers’ Forum 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
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)
  - Victoria Yan Pillitteri, FISMA Team Lead, Computer Security Division (CSD)
  - Patrick O’Reilly, Nikki Keller, and James Foti 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 7-10 days after the conference to the Forum Website [https://csrc.nist.gov/Projects/Forum](https://csrc.nist.gov/Projects/Forum)

Check FCSM website [https://csrc.nist.gov/Projects/Forum](https://csrc.nist.gov/Projects/Forum) for upcoming forum dates

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](https://csrc.nist.gov/Projects/Forum/Forum-Membership)