



2019 ASAP PRIVACY PROGRAM

June 7, 2019 – Hilton Garden Inn Downtown - Washington, D.C.

ICRM Certification Maintenance Credit – Pending; Virginia CLE – Pending; ASAP is on the IAPP List of Preferred Providers

Grand Ballroom

(Many Instructors appear in their individual capacities. The program may change based on speaker availability and budgetary considerations.)

7:30-7:55 am Registration & Morning Coffee – Visit with the ASAP Sponsors!

7:55-8:00 am Welcoming Remarks & Announcements

8:00-9:15 am Session 1.1 Keeping Pace with Technology

A panel discussion about the challenges inherent in keeping privacy programs relevant and compliant in today's ever-changing technical environment. Technology is advancing faster than it can be assessed for potential privacy implications and privacy documentation can be finalized. The panel will discuss and provide their thoughts on how practitioners might address these challenges.

Claire Barrett, Chief Privacy Officer, US Department of Transportation

Debra Danisek, Privacy Officer, US Customs and Border Protection, US Department of Homeland Security

David Lindner, Senior Director, Privacy Policy and Oversight, US Department of Homeland Security

Brian Young, Senior Counsel, National Security Team Lead, Office of Privacy and Civil Liberties (OPCL), US Department of Justice

9:15-9:20 am Stretch Break

9:20-10:35 am Session 1.2 Digital Identity and Authentication – Logging in is not what it used to be

What's the "state of the art" in digital identity and authentication? If you think it's getting a code texted to your cell phone or e-mail, or correctly identifying the last address you resided at, think again! This session will discuss new models in authentication, including those that were designed from the ground up to enhance individual privacy. Learn about where the market is heading with digital identify, the future of using your mobile device as an authenticator, and why digital identity is really just about attributes. We will also discuss the privacy benefits and risks of digital identity as well as discuss how NIST Special Publication 800-63-3, *Digital Identity Guidelines* puts privacy at the forefront of most requirements.

Jamie Danker, Director of Privacy, Easy Dynamics (formerly of DHS/NPPD)

Paul Grassi, Partner and SVP of Cybersecurity and Identity Management, Easy Dynamics (formerly of NIST)

10:35-10:45 am Coffee Break

10:45-12:00 pm Session 1.3 Privacy and the IC

When it comes to privacy, even the smallest of mistakes can have huge ramifications. In the intelligence community, this rings even louder. So what special considerations and safeguards do Privacy Officers use to ensure the safety and security of its people and systems? Panelists will discuss their policies and procedures for ensuring that privacy considerations are balanced with necessary protections.

Alex W. Joel, Chief, Office of Civil Liberties, Privacy and Transparency, Office of the Director of National Intelligence

Heather Fagan, Acting FBI Privacy and Civil Liberties Officer, Federal Bureau of Investigation, US Department of Justice

Rebecca J. Richards, NSA Civil Liberties, Privacy, and Transparency Officer

Additional Agency Representative

12:00-1:15 pm Lunch –Enjoy Lunch on your Own with Colleagues

1:15-2:30 pm Session 1.4 AI, the New Privacy Conundrum

Artificial Intelligence is the big disrupter. Programs designed for intelligent decision-making can also erode privacy on every front. What are the trade-offs, and where is the pay-off?

Brenda Leong, Future of Privacy Forum

2:30-2:45 pm Stretch Break

2:45-4:00 pm Session 1.5 Security and Privacy: A Life Cycle Approach

The federal standard is redefined. NIST Special Publication 800-37 rev.2 develops the next-generation Risk Management Framework (RMF) for information systems, organizations, and individuals, in response to Executive Order 13800, OMB Circular A-130, and OMB Memoranda M-17-25 and M-19-03. This is the first NIST publication to address security and privacy risk management in an integrated, robust, and flexible methodology. One of the key changes in this RMF update is the addition of the Prepare step, which was incorporated to achieve more effective, efficient, and cost-effective security and privacy risk management processes. Ms. Nadeau will discuss the seven major objectives of this update, as well as its objectives for institutionalizing organization-level and system-level preparation. By achieving those objectives, organizations can simplify RMF execution, employ innovative approaches for managing risk, and increase the level of automation when carrying out specific tasks.

Ellen Nadeau, Deputy Manager, Privacy Framework, National Institute of Standards and Technology, US Department of Commerce
Victoria Pillitteri, FISMA Team Lead

4:00 pm Networking Opportunity

4:30 pm Closing Remarks, Program Evaluations, Certificates of Attendance

Disclaimers & Copyright

1) Programs are subject to change. While ASAP endeavors to ensure that all its program materials are in accordance with the law and established U.S. Government policies, none of the procedures or policies presented in any ASAP training session or set forth in any ASAP publication should be considered official U.S. Government or U.S. Government Agency policy. Official policy is set forth in the appropriate directives and regulations governing each agency's activities. ASAP, its Board of Directors, Officers, employees or volunteers are not liable for any and all claims or actions that may be brought against them arising out of or relating to speaker presentations.

2) Speakers/Instructors appear in their individual capacities.

3) ASAP strongly encourages all federal government speakers who have prepared presentations under the auspices of their respective agencies, to comply with their agency guidelines in terms of making materials publically available. Participants should NOT assume that all of these presentations are available for sharing and posting on agency sites. Some presenters are not federal government employees and may retain rights to their materials. Some presenters who are federal employees may have prepared materials on their own time. All have generously given of their time to bring the best in education. If you are interested in sharing any of the presentations, please contact the ASAP office, and we are happy to work with you.

4) ASAP and any/or its suppliers shall be held harmless and will not be held liable for any consequential or incidental damages to any user hardware or other software resulting from the retrieval of program information and speaker presentations..

5) ASAP does not endorse any products or services.

6) Sharing of Information and Media Disclaimer: The names of participants registered for ASAP training **may be shared** among fellow attendees including agency/company affiliation and city/state location (as submitted for registration purposes or pulled from the database). Registrants also may specifically opt-in for email address sharing. By registering for the event, participants agree to share their name and contact information with fellow event attendees and event sponsors in order to facilitate networking among parties. This information is also shared with ASAP board and committee members for analysis purposes. Additionally, by registering, participants give permission to use photographs and video which may include them for marketing purposes including social media marketing. Those who do not wish to have their information included on the roster of attendees or appear in any photos should contact us at asap@accesspro.org.