



Information Security & Privacy Shared Interest Group

Presents

Cloud Computing Security & Privacy Considerations for Federal

May 13, 2009

Program Overview

- Presentations from expert panel on cloud computing as it pertains to security and privacy for the Federal agencies
- Identify challenges faced by government agencies as they consider adoption of Cloud Computing
- Considerations that solution providers must take into account to support Federal government requirements
- Perspectives on future direction, standards and possible solutions
- Audience question and answer session following presentations
- Slides will be posted on www.iaconline.org

Moderator – Jim Graham, SecureIT

- Committee chair for Security Governance, IAC Information Security & Privacy SIG
- More than 25 years of experience providing IT solutions and IT security professional services to Federal government agencies
- Presently Senior VP at SecureIT, responsible for delivery of Cybersecurity, Information Assurance, and Governance & Compliance services
- Prior positions include:
 - McDonald Bradley, VP/CTO responsible for solution offerings for Law Enforcement, Homeland Security, DOD C4ISR, and Intelligence
 - LEADS Corporation, VP for Information Assurance and Technology Management
 - DOMAIN Technologies, President/CEO for IT services firm that provided IT and security solutions for Law Enforcement and Intelligence organizations

Speaker Bio – Kevin Skapinetz, IBM/ISS

Kevin Skapinetz is a technology strategist and researcher at IBM Internet Security Systems, a trusted security advisor to the world's leading businesses and governments. With over ten years of experience in information security and seven years at ISS, Kevin currently works in the Office of the CTO where he is responsible for guiding the company's technology strategy with a commitment to developing business-driven products and services that preemptively protect organizations from threats. For the past two years, his focus has been in the areas of virtualization and cloud computing security. Kevin holds a computer science degree from Tulane University and a master's degree in information security from the Georgia Institute of Technology.

Speaker – Laurin Mills, Nixon Peabody

Laurin Mills is the Managing Partner of Nixon Peabody's Washington D.C. office. His practice focuses on technology, media and intellectual property litigation and counseling and white collar criminal defense. He received his J.D., cum laude, from the Georgetown University Law Center. He has B.S. and B.A. degrees from the University of Maryland. Prior to becoming an attorney, he was a marketing executive with IBM and Wang Laboratories where he was the #1 ranked account executive in the world. Mr. Mills is a prolific speaker and writer on technology-related issues. He will be a panelist at this year's "Digital Hollywood" in Santa Monica discussing the legal implications of the disruptions of many entertainment-related business models caused by the rise of the Internet and he recently briefed 30 attorneys from Google on First Amendment issues associated with the Internet and social networking sites. He is the founder and editor of Nixon Peabody's "NP 2.0" blog and wiki, which keeps a running commentary on all matters relating to digital technology and the law. He has been quoted in numerous articles concerning privacy and digital technology issues, both nationally and by international news sources such as the BBC and London Times.

Speaker – Peter Mell, NIST

Peter Mell is a senior computer scientist and Cloud Computing Project Manager in the Computer Security Division at the National Institute of Standards and Technology (NIST). He is the cloud computing and security project lead at NIST and is the lead author on NIST's upcoming cloud guidance publication. He is also the creator of the National Vulnerability Database and the Security Content Automation Protocol (SCAP) validation program. These programs are widely adopted within the U.S. government and industry and used for standardizing and automating vulnerability and configuration management, measurement, and policy compliance checking. His research experience includes the areas of cloud computing, security metrics, security automation, vulnerability databases, and intrusion detection systems (IDSs).



Cloud Computing Security & Privacy Considerations for Federal