

**Panel and Session Speaker Bios:
Spring 2014 ICAM Information Sharing Day and Vendor Expo**

Kenneth G. Calabrese
Associate Director, Office of Security and Strategic Information
Office of the Secretary
US Department of Health and Human Services

Ken Calabrese serves as Associate Director, Office of Security and Strategic Information, and Program Manager, HSPD-12. His responsibilities include management of the Department-wide HSPD-12 Program to include the Department's Identity, Credential, and Access Management Program supporting the Federal Identity, Credential, and Access Management (FICAM) roadmap; and oversight of budgets and contracts for the security directorate.

At the inception of the HSPD-12 Program, Mr. Calabrese oversaw services supporting Logical Access Control Systems (LACS) while serving under the HHS Chief Information Officer. His duties were expanded to become the Program Manager of HSPD-12 to include both LACS and Physical Access Control Systems (PACS) as part of the realignment of the HSPD-12 program under the Deputy Assistant Secretary heading the Office of Security and Strategic Information which includes the Security Directorate, Intelligence, and Counterintelligence.

Ken served as the Chairman of the Executive Steering Committee for the E-Authentication E-Gov initiative from March 2007 to February 2009.

Previous positions include serving as the Chief Technology Officer for the Department of Health and Human Services, Director of Information Management and Computer Scientist for the Army Research Laboratory, Vice President of Technology for a small information technology firm, Chief of the Information Infrastructure Support Division HQ Army Corps of Engineers, and senior management positions within the Army Corps of Engineers Central Design Agency.

Mr. Calabrese graduated Cum Laude from Loyola University of New Orleans with a BS degree in Computer Science. He graduated from the George Washington University with an MS degree in Operations Research.

He is married with four children.

Michael Daniel
Special Assistant to the President and Cybersecurity Coordinator

Michael Daniel is a Special Assistant to the President and the Cybersecurity Coordinator. In this position, Michael leads the interagency development of national cybersecurity strategy and policy, and he oversees agencies' implementation of those policies. Michael also ensures that the federal government is effectively partnering with the private sector, non-governmental organizations, other branches and levels of government, and other nations.

Prior to coming to the National Security Staff, Michael served for 17 years with the Office of Management and Budget (OMB). From September 2001 to June 2012, he served as the Chief of the Intelligence Branch, National Security Division, in a career Senior Executive Service position. This branch oversees the Intelligence Community (IC) and other classified Department of Defense programs. In this position, Michael played a key role in shaping intelligence budgets, improving the management of the IC, and resolving major IC policy issues. The branch also oversaw a variety of cross-cutting issues, including cybersecurity, counterterrorism spending, and information sharing and safeguarding.

Within OMB, Michael also served as an examiner in the National Security Division's Front Office supporting the Deputy Associate Director and in the Operations branch reviewing Navy and Marine Corps operational activities and overseas military operations such as Bosnia and Kosovo.

Since 2007, Michael has been heavily involved with Federal cybersecurity activities, starting with the Comprehensive National Cybersecurity Initiative. He has worked on cybersecurity funding issues in almost every budget since then and led an annual cross-cut review of Federal agencies' cybersecurity spending. He represented OMB on cybersecurity issues in the interagency policy process and worked with various Congressional committees and staff on cybersecurity issues. Finally, he has worked on tracking cybersecurity spending and the development of useful cyber performance metrics.

Originally from Atlanta, Michael received a Bachelor's in Public Policy from the Woodrow Wilson School at Princeton University. Subsequently, he obtained a Master's in Public Policy from the Kennedy School of Government at Harvard with a focus on International Affairs and Security. Michael also obtained a Master of Science in National Resource Strategy from the National Defense University's Industrial College of the Armed Forces in 2001.

Outside of work, Michael and his wife are raising two rambunctious boys. Michael also studies martial arts in the Chishin Ryu style with Dai Nippon Botoku Kai, a Norfolk-based karate association.

Hildegard Ferraiolo
Computer Scientist
National Institute of Standards and Technology

Hildegard Ferraiolo is a computer scientist at the US National Institute of Standards and Technology. Her research interests include identity management, mobile device security & authentication, smart cards, biometrics, public key infrastructure (PKI), and cryptography. She is the program manager for the HSPD-12/PIV program. Her recent focus is to expand the smartcard-based identity scheme to mobile devices and cloud services. She received the 2007 Department of Commerce Gold Medal.

Josh Freedman
Architecture & Interoperability Division
Office of the Program Manager, Information Sharing Environment

Josh Freedman is on detail from the Department of Homeland Security to the Office of the Program Manager, Information Sharing Environment where he focuses on ICAM-related activities across all three fabrics.

Prior to this role, Josh has worked on secure collaboration and security standards within DHS and its partners at all levels, and held positions at the Federal Bureau of Investigation and at Northrop Grumman.

Mr. Freedman holds both a Bachelor's degree and a Masters' Degree in Computer Science from Johns Hopkins University, a Masters' Degree in Program Management (IT) from George Washington University, and a Masters' Degrees in Strategic Intelligence.

Deborah Gallagher
Director, Identity Assurance and Trusted Access Division
Office of Government-wide Policy, General Services Administration

Ms. Gallagher joined the Office of Governmentwide Policy in May 2010 as part of the Identity Credential and Access Management (IDAM) office. In addition, Ms. Gallagher serves as a co-chair for the Identity, Credential, and Access Management Subcommittee (ICAMSC) and oversees the development of policies, procedures, and standards to address initiatives related to identity management, authentication, and secure access for the Federal Government. She is also responsible for the implementation of Government-wide services to support the use of the Personal Identification Verification (PIV) and PIV Interoperable (PIV I) credentials within the government as well as the Federal Public Key Infrastructure Policy Authority Chairperson. She came to GSA from the Department of Homeland Security where she worked in the Enterprise Architecture PMO in the Office of the Chief Information Officer as the lead architect for the segment architecture of the FICAM Roadmap and Implementation Guidance as well as the lead architect for the DHS ICAM segment architecture. Prior to her work with DHS, she was with the Department of Defense in the Defense Manpower Data Center where she was responsible for the integration of new technology into the DoD smart card, the Common Access Card (CAC) and implementation of functional requirements in the card issuance infrastructure. She was the PKI liaison to the Department of Defense from DMDC and played a key role on the DoD PKI Certificate Policy Management Working Group, as well as being a member of the PKI Tactical, Technical and Business working groups.

Prior to her association with DMDC, Ms. Gallagher was a representative to the DoD PKI Working groups and the DoD Information Assurance council from Defense Information Systems Agency (DISA). Her work with DISA consisted of identification of technical and functional requirements for operational and developing systems. Three years in the European Theater at DISA Europe and European Command, Comptroller provided both functional and operational experience with various systems being utilized in the DoD.

Doug Glair
Manager, Digital Identity Services
US Postal Service

Doug Glair is the Manager, Digital Identity Services in the Secure Digital Solutions organization. In this role he manages the design, development, implementation, and execution of the U.S. Postal Services' Digital Identity Services. The Federal Cloud Credential Exchange is one of the first products the Secure Digital Solutions organization is bringing to market in this space.

Prior to this role, Doug was the Manager, Supply Chain Management Strategies where he was responsible for setting and implementing Supply Chain strategic sourcing strategy, process and technology improvements. He also was responsible for managing the Postal Service's Supplier Diversity, Supplier Council, and Supplier Awards programs, as well as coordinating Supply Managements preparation and execution for SOX compliance.

Prior to joining the U.S. Postal Service in September 2008, Doug worked for Accenture helping clients improve their supply chain capabilities through process, technology, and organizational changes.

Paul D. Grant
Director, Cybersecurity Policy
Office of the Department of Defense Chief Information Officer

Mr. Paul D. Grant, a member of the Senior Executive Service, oversees the creation and maintenance of Cybersecurity Policies consistent with the objectives of the DoD CIO and national policy. The CSP Directorate oversees the DoD participation in the Committee on National Security Systems (CNSS), the Federal Identity Credential and Access Management Program, and the Executive Agent for Safeguarding Classified Information on Computer Networks (EO 13587).

In past positions, he served as Special Assistant for Federated Identity Management and External Partnering, the Director of Electronic Business and Knowledge Management and as Information Assurance Executive. He has directly supported the partnerships between the Department of Defense, the General Services Administration and other departments for cooperation on electronic government, electronic business, electronic messaging and security.

From 1996 to 1999, he was Special Assistant for eBusiness to the Deputy Assistant Secretary Defense, concurrently, serving as the DoD Co-Director of the Federal Electronic Commerce Program Office and the Federal Security Infrastructure Program Office, all homed at GSA.

Steve Gregory
Chief of the Information Integrity Branch
US Department of State

Steve Gregory is the Chief of the Information Integrity Branch within the Information Resource Management Bureau within the Department of State. His branch is responsible for the Department's Public Key Infrastructure, Anti-Virus, and Mainframe Security Programs. With regards to identity management, his PKI Program Office has grown considerably and has become a major implementer of the latest technologies to meet and anticipate federal standards and mandates related to security and identity assurance. He also serves as the co-chair for the CNSS PKI Member Governing Body and represents the Department of State on the Identity, Credential, and Access Management Subcommittee under the Information Security and Identity Management Committee of the Federal CIO Council.

Prior to joining the State Department, Mr. Gregory spent 20 years on active duty with the United States Marine Corps which he retired from in March of 2003. In addition to a Master's Degree in Computer Systems Management with an emphasis in Information Assurance, Mr. Gregory holds the Certified Information Systems Security Professional certification from the International Information Systems Security Certificate Consortium, the Certified Information Security Manager from ISACA, and the Project Management Professional Certification from the Project Management Institute.

Chi Hickey
Program Manager
General Service Administration

Ms. Hickey is currently the Program Manager for the FIPS 201 Evaluation Program. Responsibilities include testing and ensuring products related to the Physical Access Control and Logical Access Control Arena are conformant to FIPS 201 and its Special Publications. Ms. Hickey has had close to a decade of Identity Management experience including PKI, Privilege Management, Enrollment/Issuance, etc. Her previous responsibilities included supporting NSA while working at Booz Allen Hamilton, supporting DHS S&T while at Johns Hopkins University Applied Physics Lab, and directly working for DISA DoD PKI PMO.

John J. Hickey Jr.
Program Manager, DoD Mobility
Department of Defense, Defense Information Systems Agency

John J. Hickey Jr. is the Program Manager for DoD Mobility at the Defense Information Systems Agency. He is responsible for the planning, resourcing, and acquiring of commercial capability to support unclassified and classified mobility as an enterprise service. His previous assignments include Vice Director of the Defense Spectrum Organization responsibility for delivering enterprise spectrum management capability and Chief Engineer for Identity Management including both global directory services and Public Key Infrastructure.

Born in Miami, Florida and raised in northern New Jersey, Mr. Hickey has a Bachelor of Science Degree from the University of Alabama, a Master of Business Administration from Jacksonville State University and a Master in Strategic Studies from the U.S. Army War College. He served

twenty-seven years in the U.S. Army in various command and staff positions as a signal officer and an information systems engineer.

Frank Husson
Director for the Office of Emerging Technologies
US Department of Energy

As the Director for Emerging Technologies, Frank Husson leads the development and execution of Department-wide information management projects, which span multiple program lines, in order to enable the effective and efficient delivery of mission activities.

Previously, Mr. Husson was the Director of the Operational Assurance and Cybersecurity Division within the OCIO's Office of Energy IT Services, where he designed, implemented and managed the OCIO's defense in depth cybersecurity strategy.

Prior to joining DOE, Frank held multiple private sector program and project management positions providing comprehensive cybersecurity support to various federal government agencies. He was responsible for leading initiatives to develop, deploy, and manage enterprise-wide cybersecurity and incident management programs for large, diverse customers such as the National Aeronautics and Space Administration, the Department of Justice, the Department of Veterans Affairs, the National Oceanic and Atmospheric Administration, and the Federal Bureau of Investigations.

Frank received his Bachelor of Science degree in Computer and Information Science from the University of Maryland.

Naomi Lefkovitz
Senior Privacy Policy Advisor
US Department of Commerce

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), the Consumer Privacy Bill of Rights, 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 School of Law.

Leo F. Scanlon, CISSP
Director, IT Security Staff & CISO
National Archives and Records Administration

Leo F. Scanlon is currently director of the IT Security Staff and Chief Information Security Officer (CISO) for the U.S. National Archives and Records Administration (NARA). In addition to Mr. Scanlon's CISO duties, he serves as a NARA observer to the Committee on National Security Systems and the Information Security Identity Management Committee (ISIMC) of the CIO Council. He is also currently a co-chair of the ICAMSC. Prior to his service with the National Archives, Mr. Scanlon was involved in IT security issues as an independent consultant, as a systems architect in the telecommunications industry, and as a FISMA implementation specialist on major government IT projects. He is a CISSP and holds an undergraduate degree in Math Science and Technology from the State University of New York.

Dan M. Tangherlini
Administrator
General Services Administration

Dan M. Tangherlini was sworn in as Administrator of the U.S. General Services Administration (GSA) on July 5, 2013, following his 15 months of service as the Acting Administrator of GSA. Since joining the agency, he has served a vital role in President Barack Obama's agenda to build a more sustainable, responsible and effective government for the American people. GSA is responsible for improving the government's workplace by managing assets, delivering maximum value in acquisitions, preserving historic property, and implementing technology solutions.

Throughout his career, Mr. Tangherlini has been recognized for fiscal and management leadership. Before joining GSA, Tangherlini was confirmed by the United States Senate in 2009 to serve as Treasury's Assistant Secretary for Management, Chief Financial Officer, and Chief Performance Officer. In these roles, Tangherlini served as the principal policy advisor on the development and execution of the budget and performance plans for Treasury and the internal management of the Treasury and its bureaus. Tangherlini also served as the agency's Director of the Office of Small and Disadvantaged Business Utilization.

From 2006 to 2009, Tangherlini also served as Washington, DC's City Administrator and Deputy Mayor. His responsibilities included managing the day-to-day operations, budget development and performance management of District agencies. Tangherlini also served as the Director of the District of Columbia Department of Transportation (DDOT) from June 2000 to February 2006.

Prior to his appointment as City Administrator, Tangherlini served as the Interim General Manager of the Washington Metropolitan Area Transit Authority. Tangherlini also served the District of Columbia as Chief Financial Officer of the Metropolitan Police Department from November 1998 to May 2000. Before joining the District government, Tangherlini worked in the Policy Office of the U.S. Secretary of Transportation and in a variety of capacities during six years of service with the Office of Management and Budget in the Executive Office of the President.

Tangherlini received his Bachelor's and Master's degrees in Public Policy Studies from the University of Chicago and his Master's degree in Business Administration from The Wharton School of the University of Pennsylvania.

Richard L. Tannich
Senior Program Manager
US Department of Energy

Richard Tannich is a Senior Program Manager with the Office of the Chief Information Officer (OCIO), National Nuclear Security Administration (NNSA), Department of Energy (DOE). His most recent project was Director of the Enterprise Secure Network which is the Secret-level network for DOE/NNSA. As such, he led the effort to deploy the network, develop the UK Gateway, design and build the interface to the SIPRNet, establish the Computer Network Defense Service Provider, and set the PKI foundation to build the DOE ICAM initiative for the Secret fabric.

Mr. Tannich represents DOE to the Committee on National Security Systems, serves as a Tri-chair for the Sub-committee and leads the Architecture Panel comprised of five Working Groups. Realizing the need for a more comprehensive approach to the development and deployment of the DISA PKI Common Service Provider (CSP), he was instrumental in establishing the CSP Governance Board. Additionally, he is the Co-chair of the Identity Federated Coordination Working Group and is dedicated to synchronization of the various Identity Management National organizations to form a more comprehensive, long term path forward for the FICAM initiative.

J'son Tyson
Chief, Identity Credential and Access Management
US Department of Homeland Security, FEMA

J'son Tyson began his career with the Department of Defense as in 2001. He came to FEMA OCSO in the spring of 2006 in support of the HSPD-12 Program Management Office (PMO). He helped plan and execute the deployment of PIV Cards to FEMA personnel across the country. The deployment was completed in the fall of 2010 in which he helped the HSPD-12 PMO transition into the Identity, Credential, and Access Management (ICAM) PMO. J'son is the Chief of the ICAM PMO and is focusing on unifying operations, enhancing operational efficiency, and increasing security across FEMA by ensuring accurate and timely identification of personnel and resources and managing associated attributes and privileges. He is continuously assessing and improving technology, policy, and procedures to respond to the ever-changing environment and operational requirements of FEMA.

Eugene Yu
Deputy Director of Identity, Credential and Access Management (ICAM) Program
Management Office of the Chief Information Officer
US Department of Homeland Security

Mr. Eugene Yu is the Deputy Director of the Identity, Credential and Access Management (ICAM) Program Management Office at the U.S. Department of Homeland Security (DHS), Office of the Chief Information Officer.

The ICAM PMO works to assure the security of DHS facilities, people, customers, digital information and communications, and the realization of the DHS Information Sharing Environment (ISE) through the effective and efficient implementation of a robust enterprise framework for ICAM.

As Deputy Director of ICAM PMO, Eugene is responsible for defining, planning, promoting, and coordinating the enterprise implementation of the Homeland Security ICAM environment. Prior to joining DHS, Eugene spent several years providing consulting services to federal government entities on enterprise-wide IT management, cyber security, and identity and access management areas. In addition, Eugene served in the DHS Office of the Inspector General as a Senior IT Auditor where he was responsible for evaluating the Department's IT-related programs and operations to determine their level of effectiveness, efficiency, and economy. In his role, he led IT audits at DHS and briefed senior agency officials on the audit findings and recommendations.

Adam Zeimet
Acting Director/Chief Architect
US Department of Agriculture ICAM Program

Adam Zeimet is currently serving as the Acting Director and Chief Architect for the USDA's Identity, Credential, & Access Management Program. The USDA ICAM Program manages a centralized service to manage identity lifecycle & web access management for the entire USDA enterprise. The ICAM program is also responsible for providing logical access control implementation guidance. Adam has been with the program since its inception over 10 years ago and started with the implementation of USDA's enterprise 'eAuthentication' service in accordance with OMB M-04-04. Since then Adam has been involved in many aspects of ICAM, including USDA's HSPD-12 rollout, and the implementation of USDA's enterprise identity lifecycle management service.
