Panel Session:
High Impact Workforce Initiatives Redefine the Government Information Security Workforce

Moderator:

Lynn McNulty, CISSP
Director of Government Affairs for (ISC)2
Co-Chair (ISC)2 Government Advisory Board for Cyber Security

Panel Participants:

Brenda Oldfield
Department of Homeland Security
Program Director, Education & Training

Patrick D. Howard, CISSP, CISM
Chief Information Security Officer
Department of Housing and Urban Development

George R. Bieber
Chief of the Information Assurance Education, Training, Awareness and Products Branch of the INFOSEC Program Management Office (IPMO)
Defense Information Systems Agency (DISA)

Mark Wilson
IT Specialist, Information Security
National Institute of Standards and Technology

Abstract:

Coming up on the horizon are several new information security workforce initiatives that are likely to change the face of the profession, as we know it. While some initiatives are rising faster than others, it is important for the information security community to be aware of the pending changes and the likely impact they will have on government agency hiring practices, IT security roles, career paths, compensation, qualification, credentialing criteria and training requirements. In an effort to create common standards for the IT security profession, agencies such as DHS, GSA, OMB and OPM are forging ahead with initiatives that pack a powerful punch. A few of these initiatives include:

Information Systems Security Line of Business (ISSLOB)
As the April 2007 deadline for agencies to select shared service providers for security awareness training and reporting services elapses, significant questions remain regarding Tier 2 implementation of the ISSLOB Security Training requirements. Will the goals of leveraging existing workforce resources and attracting/retaining supplemental workforce resources be met by standardization?

DHS Essential Body of Knowledge (EBK) Initiative
The Education and Training Program of the National Cyber Security Division (NCSD) of DHS is leading the creation of an Information Technology (IT) Security Essential Body of Knowledge (EBK), which links competency areas and functions to IT security roles fulfilled by personnel in both the public and private sectors. Will this effort achieve its goals to characterize the IT security workforce for both private and public sectors, to establish a national skill baseline and promote

uniform training guidelines to increase the overall efficiency of IT security training? Will this DHS initiative have impact beyond the federal government?

Changes in the GS-2210 Job Series
Information security and information assurance (IS/IA) professionals recognize that their skills, knowledge and experience set them apart from information technology (IT) professionals—so why doesn't the Office of Personnel Management (OPM)? For years, the agency's occupational classification system has not recognized information security as a distinct career. However, with a growing push to create a separate and distinct job series group for the information security function, what could this mean for the profession? For its visibility? For agency budget consideration? For compensation and workforce management efficiencies?

DoD Directive 8570.1
The DoD is marching forward with its plans to ensure that the security of its mission critical information systems is overseen by a professionalized workforce through the implementation of DoD Directive 8570.1. This Directive requires all information security personnel with access to a confidential system to obtain a professional certification accredited under the global ANSI/IEC/ISO 17024 standard. Overall, the 8570 initiative is expected to affect 100,000 military and contractor personnel. Since DoD has traditionally been recognized as the standard-bearer for U.S. government security requirements, its lead with this Directive will likely be followed by other government agencies, global organizations and regulated industries. To what extent will the DoD's efforts with 8570 impact global standards of certification? What government agencies will be the next o follow suite?

Attendees of this session will learn:

- The progress of rising information security workforce initiatives and what level of impact the community is anticipating.
- How workforce initiatives such as the ISSLOB, DHS EBK DoD Directive 8570 and a potential Job Series change are affecting the way agency CISOs are planning for the future.
- The pros and cons of workforce standardization on both public and private sector IT Security personnel.

Biographies:

Lynn McNulty

Lynn McNulty brings a wealth of information security management experience in government and private practice. During his 30-year career in the federal government, Lynn was Associate Director for Computer Security at the National Institute of Standards and Technology (NIST) where his duties included policy liaison for computer security issues between NIST and other federal agencies, the Congress, and the private sector. He also played a major role in implementing the provisions of the Computer Security Act of 1987. Prior to his role at NIST, Lynn held positions as the first Director of Information Systems Security at the State Department and Security Program Manager at the Federal Aviation Administration. Lynn has positively influenced information security policy regarding everything from export controls on commercial encryption products and critical infrastructure protection to the deployment of public key infrastructure.

Since 1995, Lynn has been a consultant providing government affairs, business development and information security policy consulting services to private and public sector clients. A former member of the (ISC)2 Board of Directors, Lynn helped facilitate the establishment of the (ISC)2 organization in 1989. He currently manages government affairs for (ISC)2 and is a founding member and Co-Chair of the (ISC)2 Government Advisory Board for Cyber Security, a volunteer

group of 18 senior-level information security professionals from government and industry responsible for counseling (ISC)2 on policies, trends and certifications within the public sector. He is also a member of the Information Security and Privacy Advisory Board established by the Federal Information Security Management Act.

Lynn has been awarded the Department of Commerce Silver Medal, the Department of State Superior Honor Award and has twice received the Federal 100 Award from Federal Computer Week. In June of 2007, Lynn was awarded the 2007 Colloquium Industry Award by the Colloquium for Information Systems Security Education (CISSE) for his outstanding leadership in industry relations with information assurance education. Most recently, Lynn was named one of only three individuals to receive the exclusive Fellow of (ISC)2 designation, a distinguished honor granted by the (ISC)2 Board of Directors to those influential information security professionals who have made outstanding contributions throughout their careers to the information security profession.

Mr. McNulty is a native of Oakland California, and graduated from the Berkley campus of the University of California with a Bachelor in Political Science. He also received a Master of Arts in International Relations from San Jose State University, San Jose, California, and a Master of Science in Administration from the George Washington University in Washington, D.C.

Lynn is actively pursued by both national and local media outlets for comment as an expert source on U.S. federal government information security policy and related issues. He has been a guest on PBS's Jim Lehrer News Hour and has been featured in numerous federal IT publications such as *Government Executive Magazine, Federal Computer Week, Government Computer News, Federal Times and SIGNAL Magazine.*

George Bieber

Mr. George Bieber is Deputy, IA Human Resources and Training, Defense-wide Information Assurance Program (DIAP). In this capacity he has oversight responsibility for all aspects of the Department's IA education, training, and awareness activities, including the DoD IA Scholarship Program, as well as IA manpower and personnel issues.

Previously he was Chief, Information Assurance (IA) Education, Training, Awareness (ETA) and Products Branch, Defense Information Systems Agency. He managed the development, production and dissemination of Department of Defense (DOD) IA training and awareness materials.

Mr. Bieber has been actively involved in a wide range of Federal organizations, committees and working groups addressing IA training and professionalization issues. He has served on the Federal Information System Security Educators Association (FISSEA) Executive Board, and was the FISSEA 2000 Educator of the Year.

Patrick D. Howard

Patrick has over twenty years of experience in information security. A former Military Police Officer, Patrick successfully served in military positions in law enforcement, operations, physical security, information security, and security management, retiring from the U.S. Army in 1992. Since then he has served as an information security consultant with several government contracting firms in the Washington, D.C. area including Comsis Corp., PRC, and Troy Systems, supporting the Nuclear Regulatory Commission, US Coast Guard, Bureau of the Census, Bureau of the Public Debt, Securities and Exchange Commission, and Departments of Agriculture, Labor and Defense among others. Patrick was formerly employed as a Senior Manager for Ernst &

Young (E&Y), LLC where he developed security consulting methodologies for E&Y's national IT security practice and created policies and standards for a variety of commercial clients. He has also performed consulting services for Netigy and Quinetiq Trusted Information Management, where he was charged with developing a consultant certification program, development and delivery of CISSP preparatory training, creation of corporate security consulting methodologies, and delivery of consulting services to commercial and government organizations.
Patrick has also served as an instructor for the Computer Security Institute, has written articles on security policy development, is co-author of Total CISSP Exam Prep Book, and is author of Building and Implementing a Security Certification and Accreditation Program. Most recently Patrick was employed by the Titan Corporation and was assigned full-time to the Department of Transportation Office of the Chief Information Officer, where he served as the DOT Certification and Accreditation Program Manager.

Patrick is the recipient of the prestigious 2007 FED 100 Award for his outstanding leadership in improving IT security for the government. Patrick has a B.A. degree from the University of Oklahoma, and a M.A. from Boston University.

Brenda Oldfield

Ms. Oldfield is responsible for cyber security workforce development via training, education and professional development initiatives. In this capacity, she coordinates DHS partnerships with the National Security Agency for the National Centers of Academic Excellence in Information Assurance Education program and the National Science Foundation for the Federal Cyber Service: Scholarship for Service program.

Ms. Oldfield recently led the development of the IT Security Essential Body of Knowledge (EBK) which reflects a national skill baseline for IT security professionals. She functions as the Work Group Leader for the role-based, specialized training component of the Federal Information Systems Security-Line of Business (ISS-LOB) and she is an active member of the CIO Council's IT Workforce Committee. Brenda was recently appointed to the Executive Board of the Federal Information Systems Security Educators' Association (FISSEA).

Previously, Ms. Oldfield served as a technical training manager for a nationwide implementation of a financial and human resources information system for the federal judiciary; Overseas Technology Training Manager for the United States Information Agency; and with the U.S. Peace Corps, Regional Training Officer and then Associate Peace Corps Director (Training) in the Caribbean. Her background also includes six years as Systems Division Training Manager for a nationwide consulting firm as well as a high-school business education teacher.

Brenda earned a Masters degree in Instructional System Design from Marymount University and her undergraduate studies were in Accounting and Business Education at the University of Kentucky.

Mark Wilson

Since coming to NIST in 1992, Mark has worked on computer security program management issues, including program management reviews, vulnerability analyses and other risk management issues, and security awareness and training.

Mark served as Editor for NIST Special Publication (SP) 800-16 - *Information Technology Security Training Requirements: A Role- and Performance-Based Model* - published in April 1998. He is a co-author of another NIST Special Publication (SP 800-50) - *Building an*

Information Technology Security Awareness and Training Program - published in October 2003. He also co-authored NIST Special Publication 800-100 – *Information Security Handbook: A Guide for Managers* – published in October 2006. He is currently leading a team that is updating SP 800-16. He is also currently serving on the Information Systems Security Line of Business (ISS LOB) Tier 2 Role-based Training Working Group.

Mark also serves as the NIST Liaison to the Federal Information Systems Security Educators' Association (FISSEA), has served on the FISSEA Executive Board for six years, including two years as the Assistant Chair of the Board, and is currently the Chair of the Executive Board.

Mark came to NIST from Norfolk, Virginia where he worked for ten years in the computer security field for two U.S. Navy organizations. He earned a B.A. in political science from Old Dominion University in Norfolk in 1983. Mark is a native of New Jersey and is a U.S. Navy and Vietnam Veteran.