Panel Session:
ISS LOB Overview and Update on
Tier 1 Awareness and Tier 2 Training

Moderator:

> **Susan Hansche**
> Nortel Government Solutions/Department of State
> susan.hansche@nortelgov.com

Panel Participants:

> **Brenda Oldfield**
> Director for Education, Training and Workforce Development
> National Cyber Security Division
> U.S. Department of Homeland Security

> **Michael Smith**
> Senior IT Program Manager
> National Cyber Security Division
> U.S. Department of Homeland Security

Abstract:

During the panel discussion, Mr. Michael Smith, Senior IT Program Manager
National Cyber Security Division, U.S. Department of Homeland Security and Ms. Brenda
Oldfield, Director for Education, Training and Workforce Development
National Cyber Security Division, U.S. Department of Homeland Security will provide an
overview of the Information Systems Security Line of Business (ISS LOB) goals and also provide
an update on Tier 1 Awareness and the ongoing activities of Tier 2 Training. As a reminder the
ISS LOB goals are to:

– Identify problems and propose solutions to strengthen the ability of all agencies to identify and manage information security risks
– Improved, consistent, and measurable information security processes and controls across government
– Achieve savings or cost-avoidance through reduced duplication and economies of scale

During this panel, Mr. Michael Smith, ISS LOB Program Manager, will present an overview of the
ISS LOB goals and objectives for the Tier 1 Awareness and Tier 2 Training Initiatives. Mr. Smith
will also give an update on the ISS LOB Tier 1 Awareness program to include lessons learned
from the three shared service centers during the first year. Ms. Brenda Oldfield, chair of the ISS
LOB Tier 2 Training (T2T) working group will discuss the efforts of the ISS LOB T2T working
group to include the recommendations submitted to the Office of Management and Budget (OMB)
in December 2007 – and OMB's response. Ms. Susan Hansche, chair of ISS LOB T2T Shared
Service Providers sub-working group will discuss the current activities involved in determining
how to become a Shared Service Provider.

Biographies:

Moderator
Susan Hansche, CISSP-ISSEP
Program Manager
Nortel Government Solutions

Ms. Hansche is the director of Information Assurance Training Programs for Nortel Government Solutions in Fairfax, Virginia. She has over 18 years experience in the training field and has specific expertise in designing, developing, and implementing Information Assurance training programs for Federal agencies. For the past ten years the focus of her professional experience has been with information system security and building training programs that provide organizations with the expertise necessary to protect their information technology infrastructures. An additional expertise is in the understanding of the Federal information system security laws, regulations, and guidance required of Federal agencies. She is the lead author of "The Official (ISC)^2 Guide to the CISSP Exam" (2004), which is a reference for professionals in the information system security field studying for the Certified Information System Security Professional (CISSP) exam. Her second book "The Official (ISC)2 Guide to the ISSEP CBK" (2006) is a comprehensive guide to the Information Systems Security Engineering Model for designing and developing secure information systems within the federal government. Ms. Hansche has written numerous articles on information system security and training topics and has given many presentations at conferences and seminars.

Panelist
Brenda Oldfield
Director for Education, Training and Workforce Development
National Cyber Security Division
U.S. Department of Homeland Security

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.

Panelist
Michael Smith
Senior IT Program Manager
National Cyber Security Division
U.S. Department of Homeland Security

Mr. Smith is a senior IT Program Manager with the Department of Homeland Security/National Cyber Security Division. He is currently the Program Manager for the Information Systems Security Line of Business.

Prior to his current position, Mr. Smith was the Acting Deputy Director for Outreach and Awareness. Mr. Smith has served in a variety of other positions that include: Acting Deputy Director of Operations, US-CERT, Acting Director, Federal Computer Incident Response Center (FedCIRC), and Director Operations, FedCIRC. He has been active in the information security/assurance community since 1998. During this period, Mr. Smith has been involved in a multitude of cyber related initiatives.

 In July of 1999, he was assigned to the National Infrastructure Protection Center (NIPC) at the Federal Bureau of Investigations as the Deputy Unit Chief, Watch and Warning Unit (WWU) to assist in its organization, operation, and management. While at NIPC, he also worked to improve the process of issuing warnings of cyber-related events, and also served on the Y2K task force.

Mr. Smith served as the Deputy Manager, National Coordinating Center for Telecommunications (NCC), National Communications System (NCS). In this capacity he managed the NCC's Emergency Operations Teams, and coordinated telecommunications needs during National emergencies and disasters.

Mr. Smith has over 30 years of Federal service with experience in information technology, procurement, National Security and emergency response, cyber security, and program/project management.