

A MUST-ATTEND CONFERENCE ON...

CYBER SECURITY

EMERGING STRATEGIES, CHALLENGES, NEEDS & TECHNOLOGIES

Gain invaluable insight from **Over 20 Leading Experts** from DASD/IA, DISA, US Navy, AFCYBER(P), DHS, IATAC, US CERT, UCDDMO, DoJ, DoE, Lockheed Martin, Northrop Grumman, Raytheon, SAIC, BAE Systems, ITT, Microsoft, Intel, Symantec, VeriSign iDefense, Dasient Inc. and MacAulay-Brown, Inc.

- Latest DoD & Government Cyber Security Policies, Strategies and Imperatives
- Understanding Current Threats to DoD and National Networks & How to Defend against Them
- Emerging IT Procurement Requirements & Acquisitions Strategies
- Learn the National Vision for Critical Infrastructure Protection, including Homeland Security and Energy

Special Presentations by:

- **Mr. Bob Lentz**, Deputy Assistant Secretary of Defense for Information & Identity Assurance
- **Mr. Richard Hale**, Chief Information Assurance Executive, DISA
- **Mr. Robert Carey**, Chief Information Officer, US Navy

**SPECIAL
MILITARY
PRICING!**

Washington, D.C.
Sept. 23-24, 2009

CYBER SECURITY CONFERENCE: — EMERGING STRATEGIES, CHALLENGES, NEEDS & TECHNOLOGIES —

Last year, DoD networks suffered an onslaught of an estimated 360 million cyber attacks. As cyber attacks on US federal and commercial computer systems increase at alarming rates, the risk for national security to be compromised is also growing. Through cyber espionage and data theft, China acquired Joint Strike Fighter (JSF-35) aircraft plans. On eBay, a hard drive containing US missile defense data was for sale. Both the State of Virginia and the University of California, Berkley suffered network and database breaches to their healthcare IT systems. Critical infrastructure is being hit by an estimated 1000 or more attacks from hackers and malicious code every year. The financial and economic impacts of a one day cyber sabotage to disrupt energy infrastructure and US financial transactions is estimated at over \$35 billion USD. **The 2009 national cyber budget will be \$7 billion USD, but is that enough?** Given our ever-increasing reliance on digital connectivity, and with the reality of intensifying cyber threats from states such as China and Russia, it is a national imperative that the US directly engages these threats in order to avert potential catastrophe. This exceptional conference brings together senior level military, government and industry experts in cyber security and computer network defense to examine such questions as:

- **What are the latest DoD and Government cyber security plans, initiatives, and strategies?**
- **What is the road ahead for National Cyber Policy and Standards?**
- **What is the best course of action for mitigating the current array of cyber threats?**
- **What is being done to protect critical infrastructure from cyber and other related threats?**

Our Distinguished Panel of Experts:

Mr. Robert Lentz	Deputy Assistant Secretary of Defense for Information & Identity Assurance
Mr. Richard Hale	Chief Information Assurance Executive, Defense Information Systems Agency (DISA)
Mr. Robert Carey	Chief Information Officer, US Navy
Col Steven Hennessy	Commander, 26th Network Operations Group, Lackland AFB, USAF
Ms. Cindy Moran	Director, Network Services, Defense Information Systems Agency (DISA)
Ms. Mischel Kwon	Director, US-CERT
Mr. Gene Tyler	Director, Information Assurance Technology Analysis Center (IATAC)
Ms. Marianne Bailey	Director, Unified Cross Domain Management Office (UCDMO)
Mr. Howard Cox	Assistant Deputy Chief, Computer Crime & IT Section, DoJ
Mr. William Billings	Chief Security Officer, Microsoft Federal – US Public Sector
Dr. Eric Cole	Chief Scientist & Senior Fellow, Lockheed Martin Information Systems & Global Services
Mr. Neil Daswani	Co-Founder, Dasient, Inc.; former Security Manager, Google, Inc.
Mr. Mike Mulville	Vice President & Chief Technology Officer, SAIC Cyber Programs
Mr. Robert Frye	Senior Architect, Information Integration & Assurance, BAE Systems
Mr. Ryan Walters	Director, Security, Northrop Grumman Advanced Technology
Mr. Richard Arnold	Vice President, Washington Operations, MacAulay-Brown, Inc.
Mr. Rick Howard	Director, Intelligence, VeriSign iDefense
Ms. Audrey Plonk	Global Security and Internet Policy Specialist, Intel Corp
Mr. Robert Butts	Director, Operations, USAMS II Program, ITT Corp
Mr. Dave Gursky	Sr. Principal IA Engineer, Raytheon Integrated Defense Systems
Mr. John McCumber	Strategic Program Manager, Public Sector Group, Symantec Federal

CYBER SECURITY

CONFERENCE – EAST

Washington, D.C. • September 23-24, 2009

I. LATEST DOD & GOVERNMENT CYBER SECURITY POLICIES, STRATEGIES AND IMPERATIVES

SPECIAL ADDRESS

“Cyber Security Strategies for the 21st Century”

MR. ROBERT LENTZ

Deputy Assistant Secretary of Defense for Information & Identity Assurance

“Cyber Security in the Information Age”

MR. ROBERT J. CAREY, *Department of the Navy, Chief Information Officer (CIO)*

- Current Threats
- Balancing Access and Security
- Emerging Technologies (threats/benefits)

“Addressing the Cross Domain Information Sharing Problem in Today’s Cyber World”

MS. MARIANNE BAILEY, *Director, Unified Cross Domain Management Office (UCDMO), National Security Agency (NSA)*

“IATAC: Facilitating the Sharing of Information Critical to Information Assurance”

MR. GENE TYLER, *Director, Information Assurance Technology Analysis Center (IATAC)*

- What IATAC Provides to the DoD
- What IATAC Facilitates
- What IATAC Offers to its Customers

“Policy and Technical Solutions for Cyber Security”

MS. AUDREY PLONK, *Global Security and Internet Policy Specialist, Intel Corporation*

- How Innovation and Growth Drive Important Security Solutions
- The Impacts of Technology on Policy and Policy on Technology and How They Work Together
- Building a Triangle of Trust Between Governments, Industry and NGOs

II. CURRENT THREATS TO DOD AND NATIONAL NETWORKS & HOW TO DEFEND AGAINST THEM

SPECIAL ADDRESS

“The Latest Threats to DoD Networks; What's Being Done to Defend Against Them; and, Future Requirements for Continued and Increased/Expanded Mitigation”

MR. RICHARD HALE

Chief Information Assurance Executive, Defense Information Systems Agency (DISA)

“AF Network Defense”

COLONEL STEVEN HENNESSY, USAF, *Commander, 26th Network Operations Group, Lackland Air Force Base*

- AF Networks are Under Attack 24x7 — How are We Handling It? • What are the AF's current efforts to Improve Network Defenses? • What are the AF's Future Requirements to Improve Network Defense?

“Cyber Security Threat Landscape: Future Cyber Security Disruptors”

MR. RICHARD HOWARD, *Director, Intelligence, VeriSign iDefense*

- Underground Evolution: New Techniques Used by Cyber Cartels • Global Status by Region: Russia, China, South America, Middle East • Cyber Security Disruptors: New Threats That are at Least 5-7 Years in the Future

“The Emergence of Web-based Malware Attacks and How to Mitigate Them”

MR. NEIL DASWANI, *Co-Founder, Dasient, Inc.; Instructor, Stanford Advanced Computer Security Certification Program; former Security Product Manager and Senior Engineer, Google, Inc.*

- The Recent Fundamental Shift in how Malware is Distributed – Web Sites and Web Pages are the New Frontier • Who are the Enemies and What are Drive-By Downloads? • Data and Statistics Surrounding the Recent Distribution Trends of Web-Based Malware – and, What do these Trends Mean? • Examination of Suitable Defenses for Such Types of Attacks

“Effective Cyber Security”

MS. CINDY MORAN, *Director, Network Services, Defense Information Systems Agency (DISA)*

“A New Paradigm on Intrusion Detection”

MR. DAVID GURSKY, *Senior Principal IA Engineer, Raytheon Integrated Defense Systems*

“Cyber Cats and Mice”

MR. ROBERT FRYE, *Senior Architect, Information Integration & Assurance, BAE Systems/Network Systems C&TN*

- Kinetic Warfare / Cyber Warfare • What We Know about our Vulnerabilities & How Dependent We've Become on the Network • What We Know about Adversary Capabilities • Of Cats and Mice – They Both get Smarter and Quicker • An Uneasy (and Unstable) Cyber-Truce • Cyber Détente

“Training Cyber Warriors – What is the Impact of the Cyberspace Domain on DoD Training?”

LTC ROBERT M. BUTTS, US ARMY (ret), *Director of Omaha Operations and USAMS II Program Manager for ITT*

- After Several Years of Study, Dialog and Debate the DoD Officially Declared Cyberspace an Operational Domain and Began Laying the Groundwork (Through Strategy and Policy Development) for DoD Cyberspace Operations and a Cyber Force • In June of 2009 the Secretary of Defense Directed Commander, US Strategic Command to Create Sub-unified Command, US Cyber Command, to Carry Out the DoD Cyber Operations Mission • What is the Potential Impact of These Decisions? Who are our DoD “Cyber Warriors”? Do We Have What We Need? If Not Then How Do We Get There?



III. CYBER SECURITY AS THE CRITICAL SYSTEM COMPONENT – FROM THE GROUND UP

SPECIAL ADDRESS:

“End to End Trust”

MR. WILLIAM BILLINGS

Chief Security Officer, Microsoft Federal

- Security and Privacy Fundamentals – Building More Secure, and Privacy Enhanced Software and Services
- Technology Innovations – Three key Elements are Needed to Create Greater Trust on the Internet
- Social, Economic, Political and IT Alignment – Technology Innovations Must be Aligned with Social, Economic, Political and IT Forces to Enable Change.

“Cloud Computing, Threats, Vulnerabilities, and Security”

MR. MICHAEL MULVILLE, *Vice President & Chief Technology Officer, Cyber, SAIC*

- Cloud Perceptions
- Cloud Security Challenges
- Cloud Threats and Vulnerabilities
- Security Approaches

“Future Trends in Network Security”

DR. ERIC COLE, *Chief Scientist & Senior Fellow, Lockheed Martin Information Systems & Global Services*

- Understanding the Threat
- Prioritizing Risk
- Proactively Addressing Today’s Security Challenges

“Counterfeit and Embedded Implant Risk & Mitigation”

RICHARD D. ARNOLD, *Vice President, Washington Operations, MacAulay-Brown, Inc.*

- The Supply Chain Interdiction Threat is Real; Over 10% of IT Purchases in US are Counterfeit, and Embedded Implants Have Been Found That Prove Adversary Supply Chain Interdiction
- This Insidious Threat Defeats Perimeter and Network Monitoring, Until It’s Too Late
- Currently Available Technology Can be Used to Mitigate This Threat, and Should be a Part of an Integrated Defense-in-depth Cyber Solution

“Symantec Internet Security Threat Report”

MR. JOHN McCUMBER, *Strategic Program Manager, Symantec, Public Sector Group*

- Highlights of the Symantec Internet Security Threat Report as they Relate to the Public Sector
- How Malicious Activity is Becoming Increasingly Web-based, Fueling the Underground Economy
- Security and Data Loss Prevention Best Practices to Public Sector Agencies to Help Mitigate their Vulnerability from Internet Threats

IV. NATIONAL VISION FOR CRITICAL INFRASTRUCTURE PROTECTION, INCLUDING HOMELAND SECURITY AND ENERGY

“Critical Infrastructure Protection – Securing the Commons”

MR. RYAN WALTERS, *Director, Security, Northrop Grumman Advanced Technology*

“Botnets: The Current Threat Landscape”

MS. MISCHEL KWON, *Director, US – Computer Emergency Response Team (US-CERT), Department of Homeland Security, National Cyber Security Division (DHS NCSD)*

“Cybercrime 2009”

MR. HOWARD COX, *Assistant Deputy Chief, Computer Crime & Intellectual Property Section, Department of Justice (invited)*

- Recent Trends in Cybercrime
- International Cooperation
- Increasing Sophistication of Cyber Criminals
- Challenges Ahead