The DS Information Assurance and Cybersecurity Role-Based Training Program

Diplomatic Security Training Center (DSTC)

Dunn Loring, VA

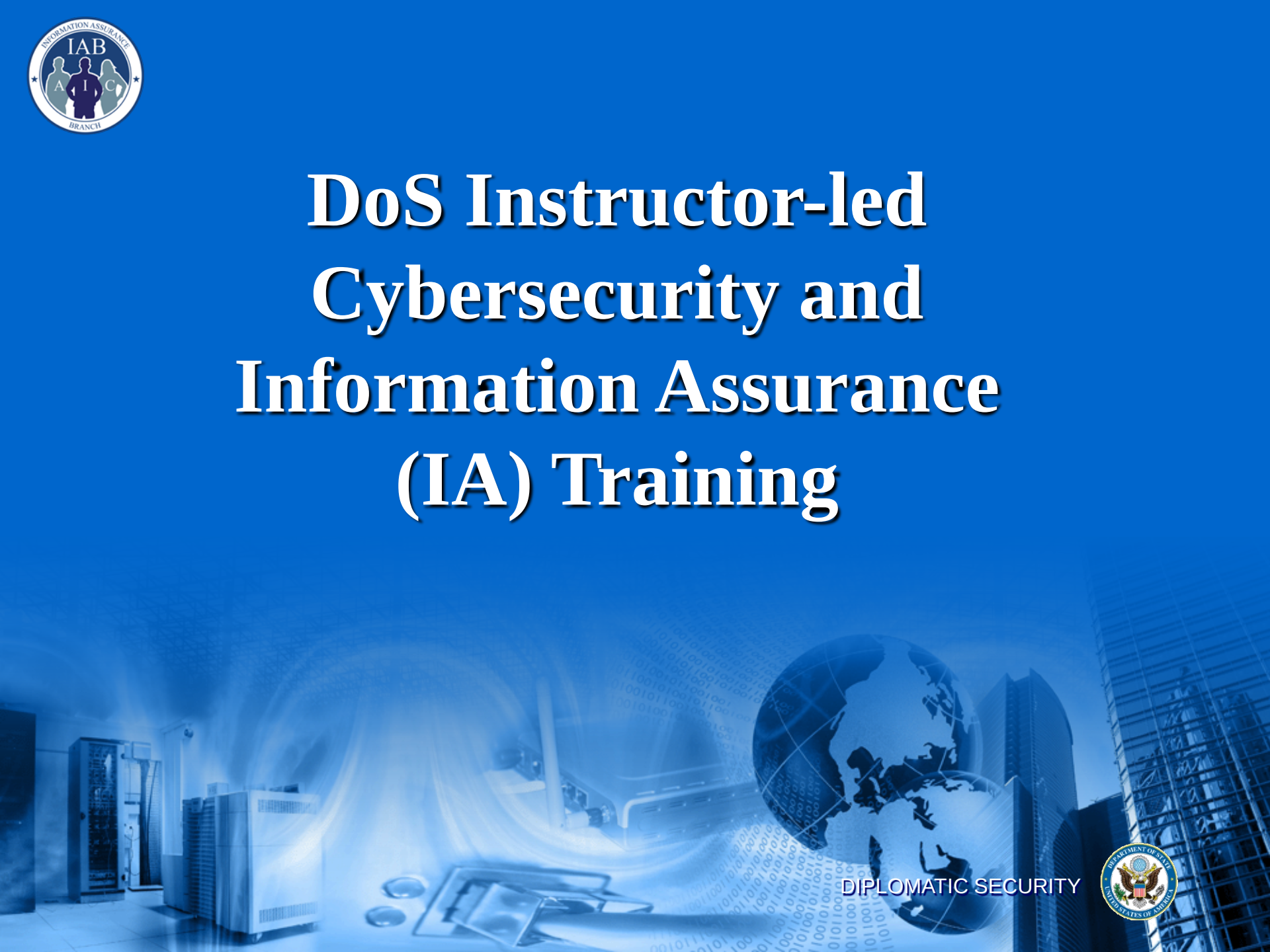
IAB Mission

The Information Assurance Branch's (IAB's) mission is to provide information assurance and cybersecurity training to U.S. Government employees under the President's and Director of National Intelligence's directives that cybersecurity is a U.S. national priority. IAB, specifically, provides Department of State role-based Information Assurance and Cybersecurity training under the U.S. Comprehensive National Cybersecurity Initiative (CNCI).

Initiatives

- Collaboration within the Department
  - DS/CS Awareness Program
  - IRM/IA
  - FSI/SAIT
  - Consular Affairs
- Collaboration with other Agencies/Departments
  - DHS – Center of Excellence
  - NIST (w/DHS) developed NICE
  - NSA – Participation in Exercises and Courses
  - FBI
  - NRC
  - SSA
  - NARA

DoS Instructor-led Cybersecurity and Information Assurance (IA) Training



DIPLOMATIC SECURITY

IAB Training

Purpose: ***Provide information assurance and cybersecurity training to U.S. Government employees under the President's and Director of National Intelligence's directives***

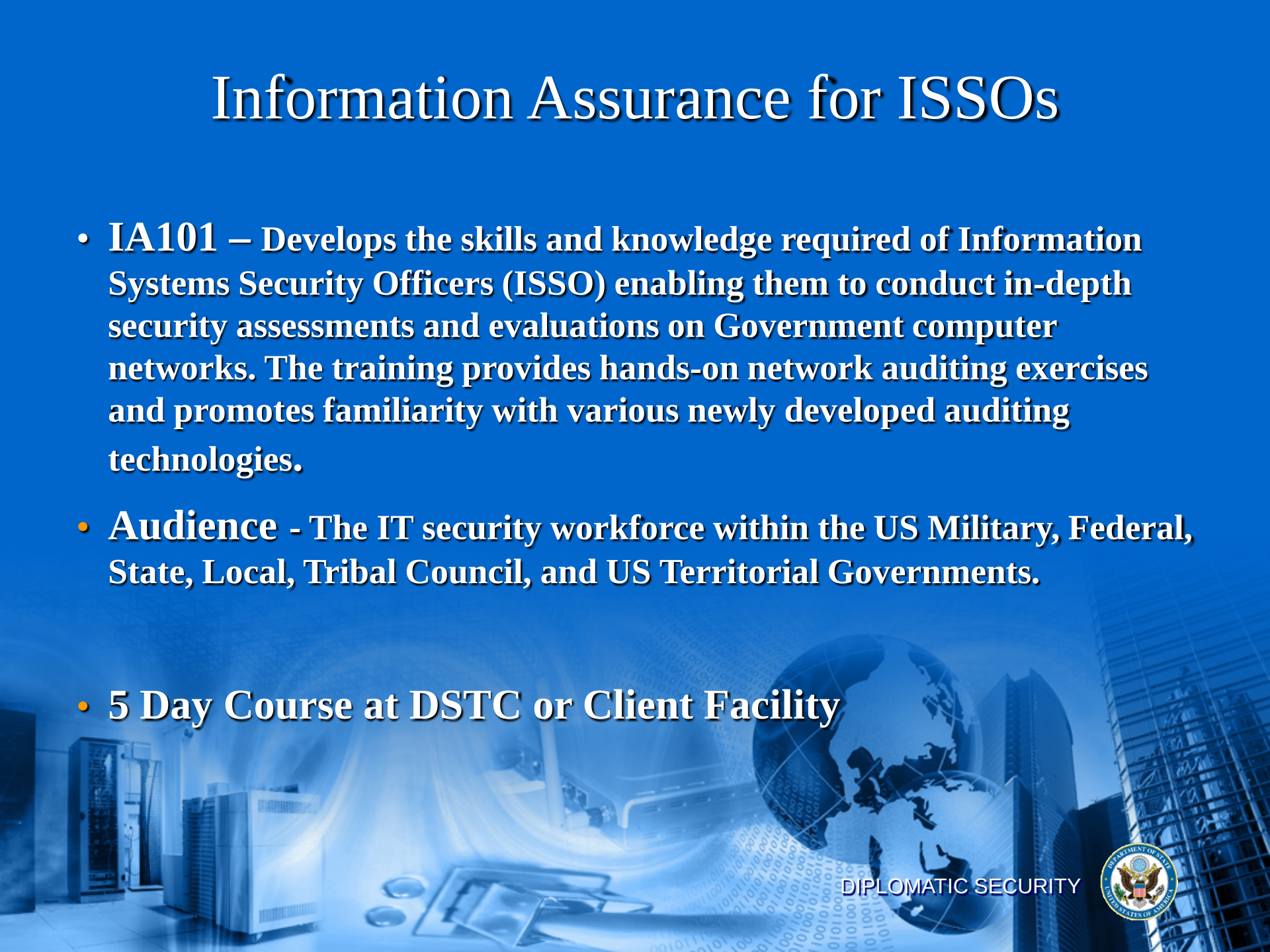
- **National Initiative for Cybersecurity Education (Cybersecurity Workforce Framework)**
- **FISMA Compliant (800-16, -34, -53)**
- **508 Compliant**
- **Federal Law Enforcement Training Accreditation (FLETA)**
- **Ongoing Course Updates**

Instructor-Led Courses

- **IA101 – IA for ISSOs**
- **IA201 – IA for System Administrators**
- **IA304 – IA for Managers**
- **IA305 – IA for System Owners**
- **IA401 – IA for Executives**
- **IA610 – IA for Developers**

Information Assurance for ISSOs

- **IA101 – Develops the skills and knowledge required of Information Systems Security Officers (ISSO) enabling them to conduct in-depth security assessments and evaluations on Government computer networks. The training provides hands-on network auditing exercises and promotes familiarity with various newly developed auditing technologies.**
- **Audience - The IT security workforce within the US Military, Federal, State, Local, Tribal Council, and US Territorial Governments.**
- **5 Day Course at DSTC or Client Facility**



Information Assurance for System Administrators

- **IA201 – Provides guidance to systems administrators on mandated network security policies and regulations that they are required to implement on the Windows operating system software used on Government networks. The training provides Best Practices security requirements and implementation procedures in accordance with the current Government security configuration requirements through hands-on exercises.**
- **Audience - Direct hire, contract personnel, and Government system administrators.**
- **5 Day Course at DSTC or Client Facility**

Information Assurance for Managers

- **IA304 – Provides training for personnel responsible for management of employees who handle sensitive information. Training focuses on manager's information security-related responsibilities to prevent and react to cybersecurity incidents within their group. Students are introduced to the risk management framework and core security principles as well as participate in scenario based problem-solving exercises and receive checklists and job aids.**
- **Audience - Government managers of employees who handle sensitive information; to include but not limited to: Management Officers and management section heads, Information Program Officers, Information Management Officers, Information Systems Officers overseas; Domestically, Program, Division, and Branch Chiefs.**
- **3 Day Course at DSTC or Client Facility**

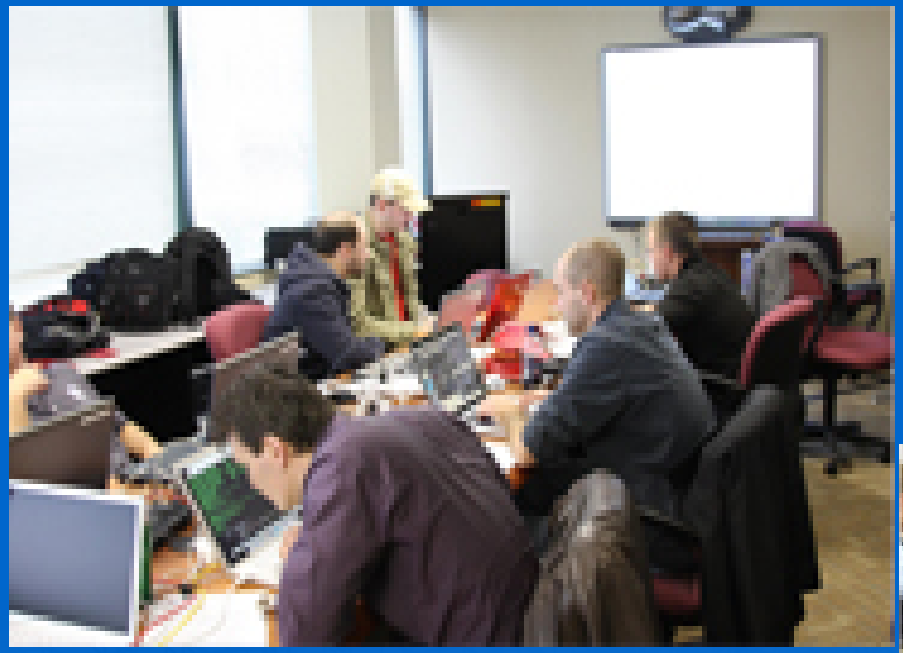
Information Assurance for Executives

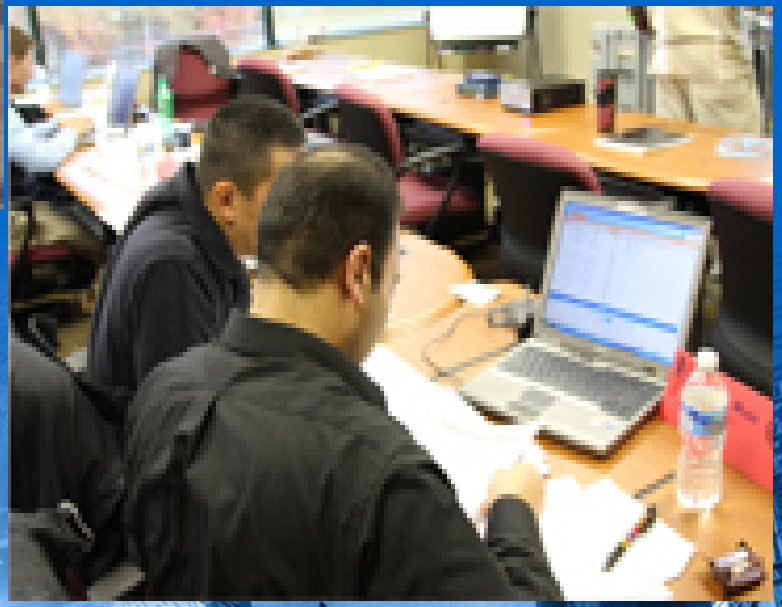
- **IA401 – Government personnel with highest level of responsibility. It includes an overview of the Government's information systems, their vulnerabilities, threats to information security and risk assessment/management. Topics include security and reporting requirements of FISMA, results of Office of the Inspector General audits and reports to the Office of Management and Budget and Congress. Case studies and lessons learned are used to emphasize the critical role of executive-level leadership in protecting the Government's information and information systems. This BP course is also available on-line.**
- **Audience - Deputy Secretary, Under Secretary, Assistant Secretary, Deputy Assistant Secretary, Senior Executive Service (SES), Executive Director, Principal Officer, and Chief Information Officer.**
- **1 Day Course at DSTC, Client Facility, or Online**

Information Assurance for System Developers

- **IA610 – Introduces application designers and/or developers to basic software assurance concepts and practices. The training provides the students with crucial resources currently available to software assurance professionals in the field, exposing the students to appropriate application security requirements, and providing hands-on experience manipulating code to mitigate weakness and prevent successful attacks. Emphasis placed on providing participants with an understanding of current threats and the specific software code vulnerabilities that they target, as well as techniques and tools used to counter these threats.**
- **Audience - Application Designers and Developers (including Web and Database Designers and Developers)**
- **5 Day Course at DSTC or Client Facility**

IAB Snapshot





Cybersecurity On-Line Learning (COL)

Purpose:

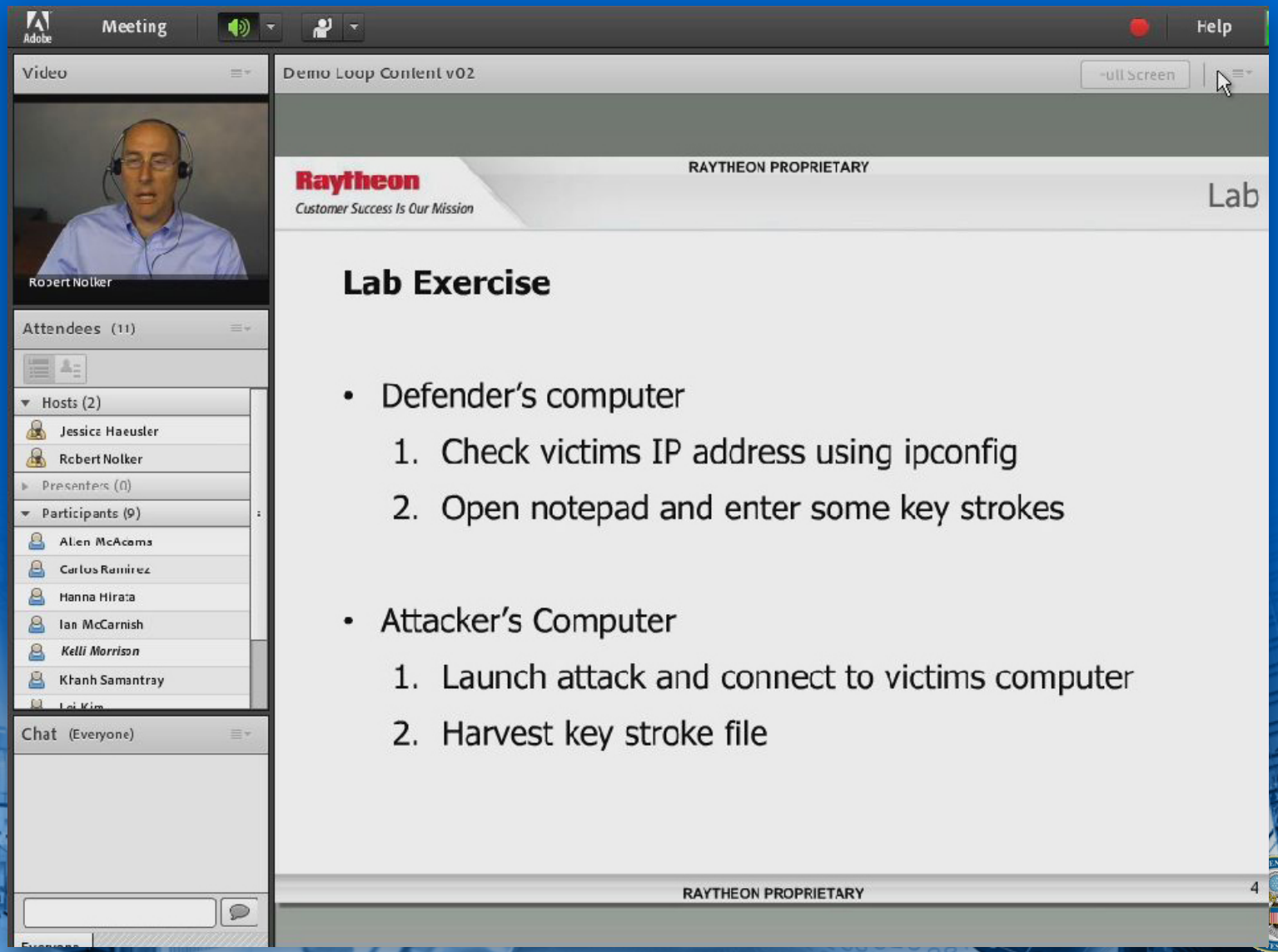
- To provide instructor-led, interactive IT security learning opportunities on a “just-in-time” basis.
- Security-related
- Provides continuous learning
- Topics that are current, interesting and helpful
- Job aids
- Interactive
- CPEs and CEUs for maintaining certifications (with organization approval)

COL Topics

- Cyber Ransom
- Cyber Extortion
- Contingency Planning
- System Attack Methods
- Introduction IPV6
- User Permissions
- BYOD Security Concerns
- Insider Threat Audits
- Windows 7 Implementation
- Application Security (I, II, III, IV)
- Stuxnet, Flame and Duqu
- eDiscovery
- Wireless Security - Roundtable Discussion
- Network Security Monitoring (I and II)
- Know Your Cyber Enemy: Environmental Virtualization

(Not an all-inclusive course list)

COL Snapshot



Information Systems Security Line of Business (ISSLOB)

- **Certification of the Diplomatic Security Training Center as an Information Systems Security Line Of Business in June 2010**
  - **Office of Management and Budget guidelines**
- **Department of Homeland Security (DHS) partnership**
- **Designation as a Center of Excellence for information assurance training**
- **Customized or Best Practices Courses**

– *"DS remains at the cutting edge of physical, cyber, and technical security."*

— Assistant Secretary of State Eric J. Boswell, DS 2010 Year In Review

Contact Information

Information Assurance Branch Chief
Caren Saxe
SaxeCT@state.gov
571-226-9743

Information Assurance Section Chief
Donald Vanderau
VanderauDon@State.gov
571-204-6118

Cybersecurity On-Line Learning (COL)
Stephan Campos
CamposSD@State.gov
571-226-9466

Cybersecurity On-Line Learning (COL)
John Light
LightJA@State.gov
703-204-6117

Information Systems Security Line of Business (ISSLOB)
Robert Clarke
ClarkeRA@State.gov
571-226-9476

DIPLOMATIC SECURITY