Innovating Security 2011

September 7 – 8, 2011 ▪ 9:00am – 4:30pm

		General User Track	Management Track	Technical Track	Additional Sessions
Wednesday, September 7					
8:00am – 9:00am	**Check-in** (HCHB 14th Street Lobby)				
9:00am – 10:00am	***Introductory Remarks, Dr. Rebecca Blank, Acting Secretary of Commerce*** **Evolving IT and Threat Landscape,** *Dr. Edward G. Amoroso, Senior Vice President and Chief Security Officer, AT&T* ***ROOM: AUDITORIUM***				
10:00am – 11:00am			**Authorizing Official Role and Responsibilities** *G. Meyer, Lead Associate, Booz Allen Hamilton* ***ROOM: 1412/1413***	**Security and Social Networking** *J. de Ferrari, Assistant Director, General Accountability Office* ***ROOM: AUDITORIUM***	**Security Certifications** *G. Bieber, Chief, IAETAP, INFOSEC Program Management Office, Defense Information Systems Agency* ***ROOM: 1414/1415***
11:00am – 12:00pm			**FISMA Forecast** *R. Ross, Project Leader FISMA Implementation Project, NIST, DOC* ***ROOM: 1412/1413***	**PANEL: Implementing Cloud Computing** **Moderator:** *J. Connor, Information Security Specialist, NIST, DOC* ***Panelists:*** *S. Leeb, NOAA, DOC* *G. Strawn, NITRD* *F. Whiteside, DOC* ***ROOM: AUDITORIUM***	
12:00pm – 1:00pm	**Lunch (on your own) and come see our special guest on** **Planning and Positioning Your Security Career,** *A. Bright, Manager, Classification and Assessment Policy, OPM* ***ROOM: AUDITORIUM***				

1:00pm – 2:00pm		**Mobile Device Security** *P. Fusco, Principal, Booz Allen Hamilton* ***ROOM: AUDITORIUM***	**Managing a Remote Workforce** *D. Campbell, Senior Advisor for Telework, USPTO, DOC* ***ROOM: 1412/1413***	**The Future of Networking** *S. Donelan, TIC Program Manager, Department of Homeland Security* ***ROOM: 1414/1415***	
2:00pm – 3:00pm			**Information System Owner Role and Responsibilities, Part I** *G. Meyer, Lead Associate, Booz Allen Hamilton* ***ROOM: 1412/1413***	**Personal Electronic Devices: Understanding the Risk** *G. Stanley, Legislative Client Advocate, National Security Agency* ***ROOM: AUDITORIUM***	**FedRAMP Overview** *M. Lewin, Director of Cloud Computing, General Services Administration* ***ROOM: 1414/1415***
3:00pm – 4:00pm			**Information System Owner Role and Responsibilities, Part II** *G. Meyer, Lead Associate, Booz Allen Hamilton* ***ROOM: 1412/1413***	**Transitional Forensics & Intrusions: Moving the Front Line** *J. Drissel, Chief Executive Officer, CyberESI* ***ROOM: AUDITORIUM***	**CSAM Training** *K. Gandola, Senior Systems Engineer, Northrup Grumman Information Systems* ***ROOM: 1414/1415***

		General User Track	Management Track	Technical Track	Additional Sessions
Thursday, September 8					
9:00am – 10:00am	**Advanced Persistent Threats,** *Mr. T. W. Sager, Chief Operating Officer, Information Assurance Directorate, National Security Agency* ***ROOM: AUDITORIUM***				
10:00am – 10:30am	***Visit the External Vendor Exhibits in the Lobby, and network with your peers!***				
10:30am – 11:30am			**The Complexities of Auditing Information Systems** *T. Zinser, Inspector General, DOC* ***(NOTE time change: 11:00am-12:00pm)*** ***ROOM: 1412/1413*** **Information System Owner Roles and Responsibilities, Part I** *G. Meyer, Lead Associate, Booz Allen Hamilton* ***ROOM: 1410***	**DOC Information Security Policy Roadmap** *P. McMahon, IT Security Policy Program Lead, OITSIT, OCIO, DOC* ***ROOM: 4830***	**Preparing for the "What If"** *B. Walsh, Acting Director, Cyber Security Program , Department of Homeland Security* ***ROOM: AUDITORIUM***
11:30am – 1:00pm	**Lunch (on your own)**				

1:00pm – 2:00pm		**Identity Theft** *S. Toporoff, Attorney, Federal Trade Commission* ***ROOM: AUDITORIUM***	**Information System Owner Roles and Responsibilities, Part II** *G. Meyer, Lead Associate, Booz Allen Hamilton* ***ROOM: 1410***	**PANEL: Implementing the Risk Management Framework** **Moderator:** *T. Ruland, Chief Information Security Officer , Census, DOC* **Panelists:** *H. Eldakdoky, Census, DOC* *J. Jackson, ITA, DOC* *L. Reed, NOAA, DOC* *R. Turk, USPTO, DOC* ***ROOM: 4830***	**Test, Training, and Exercise Programs** *D. Gallup, Lead Associate, Booz Allen Hamilton* ***ROOM: 1412/1413***
2:00pm – 3:00pm		**Protecting Government Information** *R. Shaddox, Senior Privacy Specialist, Federal Deposit Insurance Corporation* ***ROOM: AUDITORIUM***	**Assigning Position Designation** *E. Dorsey, Assistant Director, Counterespionage, OSY, DOC* ***ROOM: 1412/1413***	**PANEL: Implementing Enterprise HSPD-12 LAC** **Moderator:** *S. Sell, Logical Access Control Team Lead, NIST, DOC* **Panelists:** *E. Ebright, Federal Aviation Administration* *B. Erwin, General Services Administration* *N. Ghadiali, National Gallery of Art* *C. Irwin, National Aeronautics and Space Administration* ***ROOM: 4830***	

Innovating Security 2011

September 7 – 8, 2011 ▪ 9:00am – 4:30pm

3:00pm – 4:00pm			**Security in the Supply Chain** *D. Davidson, Chief, Outreach, Science and Standards, TMSN, DOD-CIO* ***ROOM: 1412/1413***	**PANEL: Implementing Real Continuous Monitoring** **Moderator:** *R. Clark, Senior Advisor National and Cyber Security, DOC* **Panelists:** *M. Coose, NCSD, Department of Homeland Security* *S. Solanki, BEA, DOC* *R. Turk, USPTO, DOC* ***ROOM: AUDITORIUM***	**Situational Awareness and Incident Response** *R. Slaybaugh, Cyber Threat Analyst, US-CERT* ***ROOM: 1414/1415***
4:00pm – 4:30pm	**DOC IT Priorities and Vision,** *Dr. S. Szykman, Chief Information Officer, DOC* **and Conference Wrap-up: Innovation Generation**, *Mr. T. Hurr, IT Security Compliance Officer, OITSIT, OCIO, DOC* ***ROOM: AUDITORIUM***				

Keynotes and Cross-track Discussions

Evolving IT and Threat Landscape	AT&T will provide their perspective on how information technology is evolving in the marketplace, and how this impacts the threat landscape.
Planning and Positioning Your Security Career	Learn about the efforts being performed to update the Federal Classification and Job Series for the 2210 classification series. Learn how this change impacts you as an employee in the information technology field. Understand the basic requirements and the competencies at each grade level based on the requirements of the position being filled.
Advanced Persistent Threats	Having a specific objective, threat operators are skilled, motivated, organized, and typically well-funded. Come hear how this capability and intent is affecting the Federal and National information space.
DOC IT Priorities and Vision	A perspective from the Chief Information Officer on the current and future state of the DOC Information Technology will be provided. Session will include the priorities and vision for IT within the Department.
Conference Wrap-up: Innovation Generation	Highlights of the conference sessions will be provided, and attendees afforded opportunity to provide feedback and propose ideas for innovating security within DOC.

General User Track

Mobile Device Security	As mobile devices are becoming increasingly popular, protecting the data stored on these devices becomes an even greater significance! Come learn about recent, common risks associated with these mobile devices, and techniques to protect your information. Resources to assist you will be provided.
Identity Theft	Come learn about the crime of identity theft! Attendees will learn about how you can find out if your identity has been stolen, and what steps to take if you learn that your identity has been stolen, or perhaps exposed but not yet misused.
Protecting Government Information	Talk focuses on the various types of data within Commerce, such as Privacy Act, Title XIII, personally identifiable information, etc., including data protected by non-disclosure agreements. The varied risks associated with not protecting this data will be highlighted, as well as the user and organization's role in protecting these data types.

Management Track

Authorizing Official Role and Responsibilities	The session will present an overview of the Authorizing Official role and its responsibilities as described in NIST Special Publication 800-37 revision 1. Attendance to this offering meets Authorizing Official's annual role-based training requirement. Topics include: (1) an overview of the change from "Certification and Accreditation" to "Assessment and Authorization"; (2) understanding of the authorizing decisions; and (3) key outcomes of the AA

	process to pay attention to when making risk-based decisions.
FISMA Forecast	Understand where the Federal Information System Management Act (FISMA) legislation is headed and how it may impact the enterprise! Tools and technology used for FISMA reporting requirements will be highlighted.
Managing a Remote Workforce	Come learn how the Office of Personnel Management's (OPM) new Telework Policy has changed, and gain agency perspective on real-world challenges and successes of telework. Specific focus on management tips for managing a remote workforce will be highlighted.
Information System Owner Role and Responsibilities, Part I and II	Two one-hour offerings (Parts I and II) are provided for those in the Information System Owner role. In whole, the two-part offering will (1) review the basic information system security risk management concepts; (2) review the steps in the risk management framework; and (3) describe the activities associated with each step. Attendance to both Parts I and II by Information System Owners meets their annual role-based training requirement.
The Complexities of Auditing Information Systems	Session will provide an overview of the oversight function of the Inspector General and the U.S. Government Accountability Office. The auditing process will be described, with particular focus on the complexities that information systems impose and how these complexities are changing auditing practices and reporting. A forecast of auditing priorities will be provided.
Assigning Position Designations	All positions must be designated at a position risk level commensurate with the public trust responsibilities and attributes of the position. An overview of the risk and sensitivity designations and the relationship between suitability risk levels and national security sensitivity levels will be discussed. The Office of Personnel Management's Position Designation Automation Tool will be highlighted.
Security in the Supply Chain	Session will explore the threats and challenges associated with the hardware and software supply chain, and the potential impact of such threats. Factors to consider in transforming our acquisition due diligence process for any new product or service will be highlighted. Government collaboration efforts to combat counterfeiting will also be discussed.

Technical Track

Security and Social Networking	As the leader of a GAO review of government agency actions to protect privacy and security while engaging in social networking, GAO has identified lessons learned about the need for agencies to assess risks for both privacy and security and to consider the threats posed by their use of social networking. Many agencies had not thought these through before GAO conducted a review. The results of GAO's review, including how and why the study was conducted, and the results found, will be highlighted.
PANEL: Implementing Cloud Computing	This panel discusses OU progress and challenges in implementing and managing cloud computing service offerings. Specific focus on how security issues are being addressed in offerings will be highlighted.
The Future of Networking	Gain an understanding of current and future networking initiatives and their implementation status within the federal sector. Initiatives include Trusted Internet Connection, Voice Over Internet Protocol, etc., with specific focus on Managed Trusted Internet Protocol Services (MTIPS).
Personal Electronic Devices: Understanding the Risk	Threat modeling is an established practice used to identify potential security issues. This session discusses emerging threats associated with mobile devices and proactive techniques for addressing threats.

Transitional Forensics & Intrusions: Moving the Front Line	This presentation moves beyond traditional forensics to include the analysis of malware and how this analysis can help move the engagement with the adversary outside of the target network. There will be a review of a piece of malware as an example of how this analysis helped engage the adversary externally.
DOC Information Security Policy Roadmap	The world of technology and security is constantly changing, and DOC policy must evolve to reflect changes and new requirements. Attend this session to understand the overarching factors impacting DOC policy, and the current plan for moving DOC policies forward. An example of how a security issue was identified, documented in a Corrective Action Plan, and subsequent activity for resolution will be highlighted.
PANEL: Implementing the Risk Management Framework	New changes toward the Risk Management Framework will be implemented within DOC. Gain the perspective of DOC operating units on the challenges, proposed resolutions to these challenges, and resources available for use within DOC's environment.
PANEL: Implementing Enterprise HSPD-12 LAC	Homeland Security Presidential Directive (HSPD) -12 requires a reliable, secure, and standardized form of identification for government employees and contractors. This panel session highlights efforts to implement HSPD-12, and challenges in moving toward compliance with this vision.
PANEL: Implementing Real Continuous Monitoring	The threat environment dictates the need to understand our security posture in real time. The panel discussion will provide perspective on the efforts toward automated continuous monitoring, challenges, and solutions available for use toward technology-enabled continuous monitoring reporting.

Additional Sessions

Security Certifications	An overview of security certifications will be provided in this session, including a sampling of certifications and their qualification and maintenance requirements, and how this impacts you and the DOC security workforce.
FedRAMP Overview	Understand the Federal Risk and Authorization Management Program (FedRAMP), what it does and does not offer you, and potential areas to consider when using FedRAMP to acquire cloud services.
CSAM Training	The Cyber Security Assessment and Management (CSAM) tool supports reporting and centralized storage of IT system authorization documents. Sharpen your skills by attending this session to learn more about CSAM's functionality, including tips and tricks.
Preparing for the "What If"	Cyber Storm, the Department of Homeland Security's biennial exercise series, provides the framework for the most extensive government-sponsored cybersecurity exercise of its kind. This session will provide an overview of Cyber Storm, its programmatic goals, and lessons learned. The role of DOC in Cyber Storm will be highlighted.
Test, Training, and Exercise Programs	Contingency and incident response plans assist in responding to and managing adverse situations involving IT. The session will discuss implementation of a test, training, and exercise (TT&E) program by providing guidance on designing, developing, conducting, and evaluating TT&E events so that the ability to prepare for, respond to, manage, and recover from adverse events that may affect their missions, can be improved.
Situational Awareness and Incident Response	Identifying unusual network traffic patterns and trends aids in understanding, and potentially responding to threats in real time. Learn about the US-CERT EINSTEIN Program purpose, design, and DOC's implementation. Focus will be on EINSTEIN 2 and 3.