DRAFT (DOJ, 23 NOV 2010)

INVESTIGATING LARGE-SCALE INTERNET CRIMES

OAS Sub-Regional Training Workshop for the Caribbean on Cyber Security and Cyber Crime
Antigua and Barbuda, 13-16 December 2010

Monday, 13 December

8:30	Arrival and registration	
9:00	**OPENING SESSION** Welcome and introduction by organizers and sponsors	*Antigua & Barbuda Gov't* *OAS CICTE and REMJA* *US DOS and DOJ*
9:30	**PLENARY SESSION** OAS efforts to address cyber security and cyber crime	*PANEL DISCUSSION* *Dep't of Legal Coop.* *CICTE Secretariat* *CITEL Secretariat*
10:30	Break	
10:50	**Introduction to the cyber crime track**	
11:00	**Large-scale crimes involving the Internet** The Internet has evolved into a useful tool for large-scale criminal activities • Criminal uses for the Internet: crimes, communication, and more • Criminal organizations and individuals who use the Internet • Trends and new ways for Internet-based crime • Government responses to Internet-based crime	*DOJ*
12:00	**Discussion: legal considerations for gathering electronic evidence** The law shapes the way that investigators gather evidence • Participants discuss their countries' laws and procedures for obtaining evidence and how this impacts gathering electronic evidence • Participants describe their countries' legal standards to successfully convict offenders using electronic evidence • All are encouraged to provide examples from their countries of successes and challenges in using electronic evidence in legal proceedings	*Participant discussion* *DOJ moderator*
12:30	Lunch	
14:00	**Computers, networks, and the Internet** An introduction to computer systems and how the internet works • Creating and storing information • Moving information across the Internet • Internet applications	*ATA or DOJ*
15:30	Break	

15:50	**Incident response and management: the CSIRT perspective** Much may have occurred before a crime involving computers or the Internet is reported to police • The role of the system administrator in incident response • The functions and role of the CSRIT • The goals of incident response • Assisting law enforcement in investigations **[NOTE: a DOJ or ATA facilitator will visit the cyber security track to present a law enforcement perspective on investigating cyber crime]**	*CICTE*
16:30	**Law enforcement first response: initial stages of the investigation** Investigators must respond promptly to identify and secure electronic evidence • Interviewing system administrators and other witnesses • Identifying sources of electronic and other evidence • Preserving electronic evidence • Integrating electronic and other evidence into the investigation • Case management and investigation plan	*ATA*
17:30	Adjourn	

Tuesday, 14 December

9:00	**Introduction to the group discussion problem** Participants will break into groups to apply principles presented in the workshop to a hypothetical case involving computers and the Internet	*DOJ*
9:10	**Breakout group discussions: first response and investigation plan**	*Participants separate into three groups*
10:30	Break	
10:50	**Discussion: first response and investigation plan** Participants report on their breakout group discussions, including conclusions, proposed actions, and unresolved issues	*Participant discussion* *DOJ moderator*
11:30	**User attribution: putting the suspect at the keyboard** Investigators must use all available evidence to show that a suspect was the person using the computer, creating or downloading data, and online • Direct and circumstantial evidence • Physical evidence and electronic evidence • Countering the defendant's claims that he was not at the computer	*DOJ*

12:30	Lunch	
14:00	**Collecting digital evidence: online investigations** Individuals who use the Internet leave a trail of evidence that can be hard to follow, but valuable • Common applications: e-mail, websites, IRC, IM, P2P, VOIP • Encryption • Protecting the investigator's online identity • Working with service providers • International issues	*ATA*
15:30	Break	
15:50	**PLENARY SESSION** Country reports: the current status of national cyber incident management and critical information infrastructure protection capabilities	*Country delegates from the cyber security track*
17:30	Adjourn	

Wednesday, 15 December

9:00	**Computer forensics** An introduction for investigators and prosecutors on computer forensics and the evidence available through analysis • Description of computer forensics • What forensics can and cannot provide to the investigator and prosecutor • Common techniques • Working with the forensic analyst	*ATA*
10:30	Break	
10:50	**Breakout group discussions: collecting digital evidence and creating a timeline**	*Participants separate into three groups*
12:30	Lunch	
14:00	**Discussion: collecting digital evidence and creating a timeline** Participants report on their breakout group discussions, including conclusions, proposed actions, and unresolved issues	*Participant discussion* *ATA moderator*

14:30	**Mutual legal assistance: practical considerations for improved cooperation** The global nature of the Internet requires new thinking in mutual assistance • Applying principles of international legal assistance to electronic evidence • The need for harmonized laws and procedures – Cybercrime Convention • Data preservation and the 24/7 Network • Some solutions; continuing problems • Investigator to investigator sharing • Working with service providers across borders	*PANEL DISCUSSION* *ATA* *DOJ* *Guest panelists*
15:30	Break	
15:50	**PLENARY SESSION** **Country reports: National frameworks and capabilities for combating cyber crime**	*Country delegates from the cyber crime track*
17:30	Adjourn	

Thursday, 16 December

9:00	**Discussion: putting it all together and getting to trial** Participants and facilitators share their requirements, practices, and experiences for bringing an investigation to a conclusion, preparing for legal proceedings, and success at trial	*Participant discussion* *DOJ Moderator*
10:30	Break	
10:50	**PLENARY SESSION** Enhancing cooperation and information-sharing at the national and regional levels • Law enforcement – incident manager coordination • International sharing during incident response • International sharing of electronic evidence	*PANEL DISCUSSION* *CICTE* *DOJ or ATA* *Guest speakers*
12:30	Lunch	
14:00	**PLENARY SESSION** Developing national cyber security and cyber crime strategies	*PANEL DISCUSSION* *CICTE* *DOJ or ATA* *Guest speakers*
15:00	**PLENARY SESSION** Workshop wrap-up and feedback	
15:30	**CLOSING SESSION**	
16:00	End of workshop	