

Press Release

August 9, 2010

Contact: 202-406-5708

GPA 06-10

UNITED STATES SECRET SERVICE SIGNS PARTNERSHIP AGREEMENT WITH UNITED KINGDOM OFFICIALS ESTABLISHING THE SECOND EUROPEAN ELECTRONIC CRIMES TASK FORCE

New task force to combat transnational cyber crime

(Washington, D.C.) – Creating the United Kingdom Electronic Crimes Task Force, the United States Secret Service has signed a memorandum of understanding with the Serious Organised Crime Agency. The task force, based on the U.S. Secret Service's highly successful domestic Electronic Crimes Task Force model, will be based in London, England, to provide a forum through which U.S. and European law enforcement agencies, the private sector and academia can collaborate to investigate, suppress and prevent computer-related crimes. In July 2009, The Secret Service created the first European Electronic Crimes Task Force, based in Rome, Italy.

The joint agreement, signed in London by U.S. Secret Service Assistant Director for Investigations Michael Merritt and the U.K.'s Serious Organised Crime Agency Director General William Hughes, creates new opportunities to share relevant insight, expertise and resources between the international law enforcement community to combat the transnational cyber crimes which threaten the financial security of businesses and individuals worldwide.

"The Secret Service believes that building trusted partnerships between all levels of law enforcement is the right model for facing the challenges of securing cyberspace," Secret Service Director Mark Sullivan said of the new agreement. "We believe that partnerships at the international level are essential in combating the ever-changing landscape of cybercrimes."

The Electronic Crimes Task Force (ECTF) approach developed by the Secret Service has generated unprecedented partnerships among law enforcement at the local, state, federal and, now, international level, the private sector and academia. The types of investigations handled by the ECTFs encompass a wide range of computer-based criminal activity. Examples include network intrusions, hacking cases, identity theft and other computer related crimes affecting financial and other critical infrastructures.

The Secret Service has a rich history of working collaboratively with other law enforcement agencies and believes in partnerships versus membership, where there is a strong emphasis on prevention and education, in addition to traditional law enforcement measures. The ECTF model provides a productive framework and collaborative crime-fighting environment in which the resources of its participants can be combined to effectively and efficiently make a significant impact on cybercrime. Other law enforcement agencies bring additional criminal enforcement jurisdiction and resources to the task force, while representatives from private industry and academia bring a wealth of technical expertise and research capabilities.

About the United States Secret Service

The U.S. Secret Service has taken a lead role in mitigating the threat of financial crimes since the agency's inception in 1865. As technology has evolved, the scope of the U.S. Secret Service's mission has expanded from its original counterfeit currency investigations to also include emerging financial crimes. As a component agency within the U.S. Department of Homeland Security, the U.S. Secret Service has established successful partnerships in both the law enforcement and business communities – across the country and around the world – in order to effectively combat financial crimes.

###

EDITOR'S NOTE: For questions concerning this release, please contact the United States Secret Service Office of Government and Public Affairs at 202-406-5708.