



**CTTSO**

Combating Terrorism Technical Support Office

# Investigative Support and Forensics



## Advance Planning Briefing to Industry

### 17 February 2009



# Mission

**To identify, prioritize, and execute research and development projects of multi-agency interest that provide investigative and forensic support to terrorist-related counteraction, investigations, and analysis.**



# Subgroup Membership

**EPA: NEIC**

**Federal Reserve Board**

**Intelligence Community**

**National Transportation Safety Board**

**U.S Capitol Police**

**U.S. Dept of Agriculture**

**U.S. Dept of Commerce: NIST OLES**

**U.S. Dept. of Defense: USA (CID, ISC), DCFL, DACA, DIA, USN (NCIS), PFPA, USAF (OSI), USMC (CID), SOCOM; CIFA, DCIS, NGA**

**U.S. Dept of Energy: HSS**

**U.S. Dept of Homeland Security: USSS, FLETC, ICE (FDL, FPS), SST, TSA (FAMS), TSL**

**U.S. Dept of Justice: ATF, DEA, FBI, NIJ (NCFS, NFSTC), USMS**

**U.S. Dept of State: S/CT**

**U.S. Dept of Transportation: FAA**

**U.S. Treasury Department: OIG, IRS**

**U.S. Postal Inspection Service**



# 2008 Success Stories



## Steganography Decryption

- Automated software system finds and decrypts steganography in multiple type of files and emails
- Uses distributive network attack—harnesses the unused computer processing power of a network for faster, more efficient capability
- Commercially available from AccessData as a stand alone for \$4,900 or as part of their more extensive Forensic Tool Kit package



# FY 2010 Requirements

- **R-2457 Electronic Data Recovery System**
- **R-2463 Improvised Explosive Device Defeat Tools Forensic Study**
- **R-2464 Trace Explosives Materials Collection**
- **R-2499 Advanced Log Collector**
- **R-2500 Non-Traditional Approaches to Fingerprint Development**



# R-2457 Electronic Data Recovery System

- **Develop a hardware/software data recovery system for damaged electronic devices**
- **Remove memory component from the electronic device then extract and store a copy of its data**
- **Extract volatile and non-volatile memory**
- **Read binary data from common integrated circuit types and packaging styles**
- **Contain a probe station to access data partially damaged chips**
- **Transform raw data into a usable format**
- **Software must run on Windows PC**



# R-2463 Improvised Explosive Device Defeat Tools Forensic Study

- **Conduct research to determine what exploitable evidence remains after using render safe tools on an IED**
- **Requires making exemplar devices with forensic type evidence associated with creating and handling of IEDs**
- **Submit exemplars for forensic exam before using any render safe procedures**
- **Use standard post blast collection techniques on items on which render safe tools were used and have these items forensic examined**
- **Compare results, provide best techniques, user's guide, and write a comprehensive final report**



# R2464 Trace Explosives Materials Collection

- **Produce a well researched trace explosive materials research compilation**
- **From that compilation, develop a field collection guide that includes best practices for collection and preservation of trace explosives and degradation products**
- **Develop and deliver a seminar to convey to instructors how to incorporate the findings into their training**
- **Based on subject matter expert field experience, research, and modeling**



# R-2499 Advanced Log Collector (ALC)

- **Produce an advanced computer data collector based on TSWG's previous Log Collector system**
- **Include all capabilities of previous system and add these features:**
  - **ID of all programs running in RAM**
  - **Run all features of ALC remotely over the internet**
  - **Create static binaries for Mac (OSX & higher) and Linux (RedHat) with same output as designed presently for Windows**
- **Fully operate on Windows, Mac, and Linux based computers and servers**



# **R-2500 Non-Traditional Approaches to Fingerprint Development**

- Develop a non-linear approach involving the latent print substrate as a catalyst for amplification to significantly improve the detection limit**
- Reagent should react with the more stable components of the latent print**
- Reagent should produce strong visible and/or fluorescent prints with sufficient contrast**
- Background staining of the substrate should be minimized and should not affect the print's contrast**
- Processing and development conditions should not be extreme and should make use of existing standard laboratory equipment**



# Contact Information

**BAA Specific Questions:**

**09-Q-4554@tswg.gov**