Fact Sheet: Homeland Security Information Network

Release Date: 05/28/04 00:00:00

Information Analysis and Infrastructure Protection's Homeland Security Information Network initiative is expanding its internet-based counterterrorism communications network to all 50 states, five territories, Washington, D.C., and 50 major urban areas to strengthen its real-time, collaborative flow of threat information to state and local communities.

Secure Information System

- The Homeland Security Information Network significantly strengthens the real-time, exchange of secure threat information to state and local at the Sensitive-but-Unclassified level (SBU). Future program expansion will include the county level, communication at the classified SECRET level, and the involvement of the private sector.

- The system is encrypted at the most secure levels ensuring the safest delivery of real-time interactive connectivity among state and local partners, and with the Department's Homeland Security Operations Center (HSOC) using the Joint Regional Information Exchange System (JRIES), a secure network and a suite of applications including mapping and imaging capabilities.

State and Local Information Sharing

- Each state and major urban area's participants includes governors, mayors, Homeland Security Advisor, state National Guard offices, Emergency Operations Centers, First Responder and Public Safety departments, and other key homeland security partners. Each receives software licenses, technology, and training to participate in combating terrorism, information sharing to combat terrorism and increase anti-terrorism situational awareness.

- Information sharing to reduce vulnerabilities is an essential element of the Department's mission, and this real-time flow of encrypted information between homeland security partners will allow federal, state and local agencies to better perform their jobs of protecting our nation. This increased connectivity will result in more effective communications and more efficient responses to deter, detect, prevent, or respond to terrorist actions.

Unique Capabilities

- Communications
  - Low-cost, 24/7 connectivity
  - End-to-end encrypted communications

- Collaboration/Analysis
  - Secure e-mail
  - Interactive collaboration tool (real-time, text, or voice)
  - Supports requests for information, exchange, and cross-reference
  - Search and Link/Timeline analysis, map/imagery displays

- Information
  - Daily, periodic, and ongoing report sharing
  - Suspicious incident/pre-incident indicator data
  - Media studies and analysis
  - Mapping and imaging (national, state, county, city)
  - Critical Infrastructure Protection (CIP) information
  - Strategic analysis of terrorist threats, tactics and weapons