"Homeland Security Information Network: Moving Past the Missteps Toward Better Information Sharing"

Testimony:
Captain William Harris
Delaware State Police
Criminal Intelligence Section
Delaware Information & Analysis Center (DIAC)
Commander

May 10, 2007

I am commander of the Delaware State Police's, Criminal Intelligence Section and the Delaware Information and Analysis Center (DIAC), Delaware's state fusion center. I have been asked to give you state law enforcement's perspective on the information sharing culture, as it pertains to our counter-terrorism efforts. I will specifically speak about the duplication of efforts by federal agencies that not only hamper our efforts to effective information sharing, but also hamper our efforts to secure our state and nation from future terrorist activity and attack.

I would like to preface my comments that I have had positive experiences with professionals from both the Department of Homeland Security, and many with the Department of Justice, particularly the Bureau of Justice Assistance.

As the commander of our state's fusion center, I am thoroughly familiar with the Department of Justice and Department of Homeland Security's unclassified, but sensitive information sharing systems. I would particularly like to speak about the duplication of efforts between the Homeland Security Information Network (HSIN), the Regional Information Sharing System (RISS), and Law Enforcement on Line (LEO), to include INFRAGARD.

The RISS network was established in 1974 and has been a staple of federal, state, and local law enforcement information sharing for over 30 years. In 2002, RISS launched new assets with the Automated Trusted Information Exchange. This new asset was to enhance the information sharing environment with those non-law enforcement, homeland security stakeholders, within their own discipline, cross discipline, and their local, state, and federal law enforcement partners.

Each of the previously mentioned systems offer similar capabilities such as an electronic bulletin board, document library, a chat tool, and encrypted Email. As a law enforcement agency participating in the information sharing environment, we forced to choose between information sharing systems with separate logons and passwords, and the monitoring of those systems. Because of this bureaucracy of multiple systems, our personnel have had to monitor all of these systems in an attempt to stay current on the sharing of counter-terrorism and homeland security information.

This has also forced law enforcement agencies, such as mine to look at the best information sharing resource available. This has been by far the Regional Information Sharing System (RISS). This system is both robust, user friendly, and contains more relevant, reliable, and timely law enforcement and homeland security information that is actionable for the line level law enforcement personnel, that will most likely be the identified link to disrupting pre-operational planning of a domestic or international terrorist.

The RISS network gives access to an electronic bulletin board (RISS Leads) used by multiple law enforcement agencies, to include a national criminal intelligence database (RISS Intel) to include gangs (RISS Gang). In addition to this RISS has connectivity to assets such as the High Intensity Drug Trafficking (HIDA) Centers (19 databases), the National White Collar Crime Center, the U.S. Secret Service's Targeted Violence Information Sharing System (TAVIS database), the Law Enforcement Intelligence Unit (LEIU database), the El Passo Intelligence Center, (EPIC database), the National Drug

Pointer Index (NDPIX database), to name just a few. These features are the force multiplier that law enforcement agencies and fusion centers are searching for to assist in identifying anomalies and those common crimes and networks that are part of pre-operational planning by both domestic and international terrorist.

Duplication of systems within the information sharing environment with the public and private sectors are just as confusing and bureaucratic. HSIN has several portals for this purpose, the FBI is promoting INFRAGARD as a communication tool, and RISS has the Automated Trusted Information Exchange (ATIX). The concept of including the public and private sector are part of the Information Sharing Environment Implementation Plan, and makes good business sense to include these disciplines. However, when working with our critical infrastructure stakeholders in the private sector, they are presented with three systems that are supposed to accomplish the same goal.

Once again, state and local law enforcement, which have responsibility for protecting our critical infrastructure, are forced to choose the best information sharing resource available. This has been by far the RISS ATIX system, for many of the same reasons law enforcement likes the features of the RISS law enforcement network. The information, contacts, and features available on the ATIX system make it more robust and user friendly. Additionally, like HSIN, users have the ability to go into their identified "communities" or disciplines, however unlike HSIN and INFRAGARD; users have the ability to gather information and contacts from users outside of their discipline, giving them relevant, reliable, and timely information sharing relationships of mutual value. This was most evident recently in February 2006, when DHS released the "lessons learned" from "Cyber Storm," a cyber security preparedness exercise. One of the key lessons learned, was to no one's surprise, that interagency coordination and cross-sector information sharing enhanced overall coordination, communication, and response. RISS ATIX gives our law enforcement personnel and key stakeholders within our state and region this type of effective information sharing capability that no other system does.