

**Testimony of John D. Cohen
President & CEO, PSComm, LLC
Before the House Government Reform Committee's
Subcommittee on Technology, Information Policy,
Intergovernmental Relations and the Census
May 20, 2003**

**Can the Use of Factual Data Analysis
Strengthen National Security? – Part Two**

Introduction

Good morning Chairman Putnam, Vice Chairwoman Miller, Ranking Member Clay and other distinguished members of the subcommittee. Thank you for this opportunity to participate in this critically important hearing.

The comments and observations I offer today are based on having spent my entire career – close to 20 years – involved in law enforcement operations, oversight and policy development. My views on this issue come from a somewhat unique experience base that includes service as a:

- Special Agent in the Office of Naval Intelligence;
- Police officer who regularly worked side by side with federal agents to conduct investigations of international criminal organizations;
- Senior investigator for a Congressional committee that conducted oversight reviews of our nation's intelligence and law enforcement efforts;
- Policy advisor to the Director of the Office of National Drug Control Policy; and
- A homeland security advisor who has helped a number of city and state governments assess and improve their ability to detect, prevent and respond to acts of terrorism.

First, let me clearly state that if we as a nation are truly serious about preventing acts of terrorism, we have to dramatically improve the flow of information among federal, state and local law enforcement entities. We also need to enhance our ability to provide front line law enforcement personnel (whether they are investigators assigned to a joint terrorism task force or beat cops) with accurate, timely and useable information. This was an issue prior to the attacks of 9/11 and as we all know, our inability to “connect the dots” was identified during the post-attack inquiries as a significant problem.

It is now almost 20 months after the attacks of 9/11. Yet despite universal recognition of the problem, we have not taken the necessary steps to establish a national law enforcement information sharing capability that facilitates the collection, analysis and dissemination of law enforcement information so that we can “connect the dots.” This represents the most serious impediment to our nation’s efforts to prevent violent crime and stop future acts of terrorism.

Data mining or factual data analysis can serve a critical role in strengthening both day-to-day crime prevention and homeland security. We need to clearly define what type of information would be most valuable in accomplishing that goal and what type of systems would best support our efforts to stop future terrorist attacks. And we need to do this now, as we begin investing finite tax dollars into researching, developing and implementing complex, new electronic monitoring and detection tools that allow law enforcement to discover the activities of potential terrorists. That is why Mr. Chairman, I congratulate both you and this Committee for holding hearings on an issue that I believe is at the heart of our nation’s ability to protect the public.

Where are we today?

After almost 20 months since the attacks on the World Trade Center and the Pentagon, the view from government officials who serve at the front lines of our domestic war on terrorism is that very little has changed from the perspective of information sharing. In some ways things have gotten worse.

Prior to the events of 9/11, information sharing among law enforcement agencies was based on personal relationships. When I was a police officer, we used to have a saying: “Cops share information; agencies don’t.” What this means is that if a police officer from one agency happens to have a good relationship with a cop from another (or even a local FBI agent), then there is a mechanism for the sharing of information about investigations and other relevant issues. Absent that type of relationship, information sharing was often more difficult. But even when the sharing of information did occur, it involved phone conversations, faxes or traveling to meetings to exchange paper documents. Because there was no infrastructure to support the sharing of key investigative type information, it was often left to individual law enforcement personnel to establish the mechanisms and, in some cases, the information systems that facilitated the exchange of information. In the late 1980s and early 1990s, the emphasis was placed on establishing pointer index-type systems so that if one police officer had a name or an address of interest, he or she could be directed to an investigator in another agency who may have additional valuable information.

Recognizing that information sharing through phone calls, meetings and faxes was not truly an effective way to facilitate data mining, information analysis and therefore the solving and prevention of crime, the late 1990s saw growing interest in the establishment of “integrated justice” systems. These systems linked federal, state and local criminal justice information, so that information could be shared electronically and proactively. At the same time, police agencies began to focus on moving away from the reactive strategies that drove police operations. They started to become more information driven and proactive. Many police agencies set a goal to enhance their ability to prevent crime by analyzing crime and other related data, identifying emerging crime problems and implementing operational strategies designed to prevent situations from escalating into emergencies. Thus began the process known as COMPSTAT.

Post 9/11, the sharing of information between law enforcement has at best remained the same but in some respects has become more difficult.

Arguably, there is greater recognition throughout the law enforcement community that information sharing is important. And in those jurisdictions in which strong interpersonal relationships exist, information sharing continues to be positive. But in those areas of the country where interpersonal relationships do not exist, information sharing is not as effective. The result is ad-hoc and inconsistent information sharing and cooperation among law enforcement entities.

More importantly, despite a tremendous amount of rhetoric, there has been little to no progress in establishing a truly integrated law enforcement information system that facilitates the flow and analysis of information among the nation’s law enforcement agencies.

- Many police, public health entities, parole officers and courts are operating with 20-year-old information technology.
- Even though high-speed digital technology is currently available, many police officers still wait long periods to receive basic information about a vehicle or person they stop.
- In some states, days or weeks may pass before criminal warrants find their way into state databases, leaving dangerous criminals on the street and police without this information.
- In many states, judges might sentence offenders with outdated information regarding their criminal history records.
- In most states, investigators in one jurisdiction may be unaware that information regarding an individual under investigation exists in a neighboring jurisdiction.

- The General Accounting Office reports that the 12 terrorist related watch lists maintained by various federal agencies are still maintained in stove-piped or non-linked information systems.
- Brian David Mitchell, the suspect in the Elizabeth Smart kidnapping case, spent six days in a San Diego jail, but was released because Utah authorities had not notified other law enforcement agencies that he was a suspect. And, it wasn't until a month later after the suspect was arrested, that authorities matched his fingerprints.
- During the three weeks when two snipers terrorized the Washington, D.C. area, various local police agencies stopped the vehicle containing both suspects on 10 separate occasions. Even though police ran the license plates through the national database, there was no record that the car had been stolen or its occupants were wanted for any crime.
- Even worse, weeks before the first sniper attack, a latent fingerprint of one of the alleged snipers was retrieved at the scene of a robbery homicide in Montgomery, Alabama. State officials in Alabama were unable to make the connection, because they were unaware that the fingerprint was on file with the federal government. Alabama only maintains a statewide crime database; it is not linked to the system that maintains federal information. Authorities only learned the truth when one of the sniper suspects told police about the robbery in Alabama, and a paper copy of the latent print was transported to Washington, D.C. and entered into the federal system. If the identification had occurred in a timelier manner, a felony warrant would have been placed into the National Crime Information System (NCIC). Then, Montgomery County, Maryland police, who stopped a vehicle containing both suspects four hours prior to the first sniper shooting, could have made arrests. The sniper attacks would never have occurred.
- While the sniper attacks were ongoing, information received through a tip line had to be hand written on slips of paper and sent by fax or retrieved, because no electronic information system existed.

The fact that the information systems used by individual law enforcement agencies are not inter-linked directly impedes our ability to prevent future terrorist attacks. It is hard to believe that greater emphasis has not been placed on establishing "integrated justice" systems at a time when billions of dollars are being provided to federal, state and local governments in the name of homeland security. Perhaps the reason why is because for the most part, the federal government considers the role of state and local governments as that of "first

responders,” ignoring the fact that state and local law enforcement play critical roles in detecting and preventing acts of terrorism.

Additionally, the Department of Justice has established an artificial separation between counter-terrorism and crime prevention efforts. Domestic terrorism is viewed as more of an intelligence issue, requiring separate processes and protocols than day-to-day crime fighting efforts.

The philosophy that somehow counter-terrorism is a domestic intelligence issue; crime is a law enforcement issue and both need to be treated separately is not only inefficient but also dangerous.

The first indication that a terrorist cell is operating within the United States may not come from information uncovered as part of an intelligence operation, but instead it may come from behavior discovered during an investigation by state or local police, looking into suspicious activity. We know that terrorists often use traditional crimes such as drug and illegal weapons trafficking, money laundering and bank robbery to offset costs and further support their political/terrorist objectives. Therefore, rapidly collecting and disseminating solid information about the people who commit crimes and the places where crime is committed is essential to our homeland security efforts.

Additionally, terrorists are dangerous, not because they say or believe dangerous things, but because their beliefs motivate them to commit acts of violence targeting people, places and things. These acts of violence – whether motivated by political or religious ideology – are still criminal acts. Is a mass murder that is motivated by political ideology any more sinister than a mass murder motivated by greed or mental illness? Preventing any act of violence within the United States should be a top priority, regardless of whether motivated by greed, criminal intent or ideology. Even prior to passage of the USA Patriot Act, mechanisms were in place to facilitate the sharing and use of sensitive intelligence information by domestic law enforcement agencies. These procedures and rules ensured that sources and methods were protected, while at the same time, dangerous criminals could be identified, investigated and prosecuted in a manner that respected the fundamental constitutional protections of all Americans.

Where do we go from here?

The loss of life and financial repercussions that would result from a successful terrorist incident requires that state and local governments do whatever they can to prevent such an attack from occurring. In this regard, state and local homeland security efforts must become information driven, proactive and focused on preventing future attacks.

These preventative efforts can supported by:

- Providing training to state, local and tribal law enforcement, public health and other government personnel, so that they are better able to identify signs that a terrorist group is operating within their midst; and
- Collecting, analyzing, and disseminating critical information so that beat cops, detectives, state troopers and other law enforcement personnel – regardless of their assignment – are better able to identify terrorist group operations.

A key component of any effort to protect the public from international terrorists or homegrown criminals is the rapid access by law enforcement and other appropriate personnel to information contained in local, state and federal databases. Currently 38 states and the District of Columbia have begun efforts to create “integrated justice” information systems, linking police, courts, corrections and other criminal justice components. These systems will allow for the rapid flow of information about the people who commit crimes and the places where crime occurs. Law enforcement officials and policy makers will be able to identify suspicious and unusual trends and develop information-driven strategies that effectively target criminals and the conditions that facilitate criminal activity. These same systems are essential components of any organized effort to prevent or respond to future critical incidents and terrorist threats. They also form the backbone for daily operations.

Accordingly, before the country invests millions of dollars creating a system that allows the government to track credit card information of innocent Americans, we need to make it a priority (and homeland security funding should be available) for each state to link the independent information systems used by city, county and state criminal justice entities to allow for the rapid flow of information about the people who commit crimes and the places where crime occurs. These statewide systems should then be linked to federal systems. This information sharing will support efforts by law enforcement to identify suspicious trends and effectively target those involved in criminal activity.

But, it is not enough to link law enforcement systems. Public safety information and communication systems must be interlinked with those of other state and local government systems (those that support emergency management, transportation, public health, social service and public utility related activities). State and local departments work daily with each other, but often this work is hindered by “stove piped” information systems. Improving each state’s information technology

infrastructure will dramatically improve the ability of federal, state and local governments to identify emerging homeland security related or other public safety and public health threats.

These efforts should include establishing aggressive oversight of law enforcement and homeland security related activities. While the vast majority of law enforcement officers are honorable men and women doing a job that most people would be unwilling and unable to do, there are and will be those unethical individuals who will abuse the authorities entrusted to them. As we expand the universe of information available to law enforcement, we also expand the potential for abuse. I am hopeful that Congress, the courts and the media will continue to fulfill their vital oversight responsibility to uphold and protect the privacy rights and civil liberties of all Americans.

In conclusion, factual data analysis will strengthen national security, but only when critical law enforcement systems have been inter-linked – a preliminary step that to this date has not been.

Thank you for the opportunity to participate in this hearing.