Department of Justice

STATEMENT

OF

RICHARD A. MCFEELY
SPECIAL AGENT IN CHARGE
BALTIMORE FIELD OFFICE
FEDERAL BUREAU OF INVESTIGATION

BEFORE THE

COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

AT A HEARING ENTITLED

"BUILDING SAFER COMMUNITIES: THE IMPORTANCE OF EFFECTIVE FEDERAL-LOCAL COLLABORATION IN LAW ENFORCEMENT"

PRESENTED

JUNE 20, 2011

Statement of Richard A. McFeely
Special Agent in Charge
Baltimore Field Office
Federal Bureau of Investigation

Committee on the Judiciary
United States Senate

"Building Safer Communities: The Importance of Effective Federal-Local Collaboration in Law Enforcement"
June 20, 2011

Good morning, Chairman Leahy and Senator Coons. Thank you for the opportunity to appear before you today to discuss the FBI's coordination with federal, state, and local law enforcement here in Wilmington and across the country.

Since September 11, 2001, the FBI has shifted from a traditional crime-fighting agency into an intelligence-led, threat-driven organization, guided by clear operational strategies. Today's FBI is focused on predicting and preventing the threats we face while at the same time engaging with the communities we serve. This shift has led to a greater reliance on technology, collaboration, and information sharing.

The Baltimore Field Office of the FBI has jurisdictional responsibility for the State of Delaware where we maintain two Resident Agency (RA) offices. These RAs are responsible for all of the FBI's information sharing and investigative work in Delaware. In addition to task force participation, a number of special agents in Delaware serve in an official liaison role and coordinate with federal, state, and municipal law enforcement agencies. Some of these agents are regularly embedded with the partner agencies, where they facilitate the efficient and frequent exchange of information and work to better understand the intelligence needs of FBI partners.

There was a day in law enforcement when teamwork and partnership were virtues. Today, they are absolute necessities. Also of great necessity is the ability to share real-time information that allows both the FBI and its partners the world over to cross jurisdictional boundaries and quickly 'connect the dots' when every minute counts. Gone are the days when information was held onto for fears of compromising investigations; the benefits of full and open sharing with our partners has proven time and time again to be more valuable than the close holding of intelligence.

<u>Information Sharing</u>

The FBI has two strategies we rely on to push information out to our partners: one is a formalized structure and the other is informal and tailored to each individual jurisdiction.

From a formalized perspective, the FBI's National Information Sharing Strategy (NISS) ensures that information is shared as fully and appropriately as possible with federal, state, local, and tribal partners in the intelligence and law enforcement communities. The NISS is based on the principle that FBI information and information technology systems must be designed to ensure that those protecting the public have the information they need to take action.

The NISS includes three components: Law Enforcement National Data Exchange (N-DEx); OneDOJ; and the Law Enforcement Online (LEO) network.

For its part, N-DEx provides a nationwide capability to exchange data derived from incident and event reports. It serves as an electronic catalog of structured criminal justice information—such as police reports—that provides a "single point of discovery;" leverages technology to relate massive amounts of data that is useful information; automates discovery of patterns and linkages to detect and deter crime and terrorism; and affords enhanced nationwide law enforcement communication and collaboration.

The process of connecting the dots between seemingly unrelated pieces of criminal data housed in different places is the backbone of N-DEx. The system enables its law enforcement users to submit certain data to a central repository—located at our Criminal Justice Information Services (CJIS) Division in West Virginia—where it is compared against data already on file from local, state, tribal, and federal agencies to identify links and similarities among persons, places, things, and activities across jurisdictional boundaries. The State of Delaware is a full partner in the N-DEx project.

OneDOJ enables the FBI to join participating federal, state, tribal, and local law enforcement agencies in regional full-text information sharing systems under standard technical procedures and policy agreements.

Lastly, the LEO network provides web-based communications to the law enforcement community to exchange information, conduct online education programs, and participate in professional special interest groups and topically focused dialogue. It is interactive and provides state-of-the-art functions such as real-time chat capability, news groups, distance learning, and articles on law enforcement issues.

LEO started in 1995 as a small dial-up service with just 20 members. Now, it has more than 100,000 members across the world and a host of features and capabilities offered through a Virtual Private Network on the Internet.

LEO offers many tools that cross-cut all law enforcement agencies on a global basis. There is no other on-line service that matches its capabilities. For example, LEO hosts the eGuardian system, which is a sensitive but unclassified (SBU) information sharing platform developed to help meet the challenges of collecting and sharing terrorism-related activities amongst law enforcement agencies across various jurisdictions. It allows law enforcement agencies to combine new suspicious activity reports (SARs) along with existing (legacy) SAR reporting systems to form a single information repository accessible to thousands of law enforcement personnel. The information captured in eGuardian is also migrated to the FBI's internal Guardian

system, where it is assigned to the appropriate Joint Terrorism Task Force (JTTF) for any further investigative action.

LEO is also home to the Virtual Command Center (VCC). In Delaware, I have made the VCC the main centerpiece of our strategy to share information in a major crisis. VCC provides an "Events Board" feature which allows information to be posted as the event occurs and allows us to post photographs, scanned documents, and any information deemed pertinent to the crisis. Whatever agency is hosting the VCC can allow access to individual persons or entire agencies if needed. Critical Incident Managers, such as emergency planners, now can remotely have access to a crisis without having to be on-scene.

The FBI is a participating member of the Law Enforcement Coordinating Committee (LECC) in the District of Delaware. The LECC serves as a catalyst for forging partnerships with federal, state, and local law enforcement and prosecutors.

But our commitment to information sharing does not stop with our law enforcement partners. The FBI-sponsored InfraGard brings together representatives from the private and public sectors to help protect our nation's critical infrastructure and key resources from attacks by terrorists, criminals, and others who would do us harm. It is a partnership that makes sense, since most U.S. infrastructure components—like utility companies, transportation systems, telecommunication networks, water and food suppliers, public health, and financial services—are privately owned and operated.

The following are just a few examples of the FBI's efforts to share information and leverage all available resources and expertise to combat the threats posed by terrorism and criminal enterprises.

Counterterrorism

As one of the few members of the U.S. Intelligence Community with a combined law enforcement and intelligence mission, the FBI serves as a critical link between the intelligence and law enforcement communities in the United States. We are committed to working together to prevent both crime and terrorism, here at home and with our partners around the world.

In Delaware, the FBI maintains a Joint Terrorism Task Force (JTTF) in the Wilmington RA. In addition to FBI agents, there are full-time Task Force Officers (TFOs) from partner agencies, including the Delaware State Police (DSP), U.S. Immigration and Customs Enforcement (ICE), Bureau of Alcohol, Tobacco and Firearms (ATF), Wilmington Police Department (WPD), Delaware Department of Corrections (DOC), and Delaware Division of Alcohol and Tobacco Enforcement (DATE). Each of the JTTF TFOs has the necessary credentials and clearances required to fully participate. In total, twelve agencies participate and contribute to the Task Force.

While JTTFs are certainly considered part of the FBI's formalized information sharing strategy, many of our successes over the recent years have come from the benefit of co-location and direct outreach to our federal, state and local partners. For example, recognizing that much of the work

of the FBI and the rest of the Intelligence Community are within a classified information environment, I have offered every Police Chief in Delaware the opportunity to apply for a SECRET security clearance. This is a vital part of our local information sharing strategy because every month, we bring in all the cleared Chiefs and provide a classified threat briefing, including: (1) timely Homeland threat reporting; (2) threat trend analysis; (3) information about specific terrorist groups and extremist activities; and (4) current investigations of the Baltimore JTTF.

Cyber Crime

We have cyber squads in each of our 56 field offices around the country, with more than 1,000 specially trained agents, analysts, and digital forensic examiners. Together, they run complex undercover operations and examine digital evidence. They share information with our law enforcement and intelligence partners and they teach our counterparts—both at home and abroad—how best to investigate cyber threats. The Wilmington RA has agents specifically designated for cyber investigations with extensive specialized training. In complex cyber cases, additional resources are provided by the Baltimore Field Office and FBI Headquarters.

Between 2008 and 2011, FBI Agents in the Wilmington and Dover RAs, working in coordination with the DSP High Tech Crimes Unit (HTCU), successfully investigated cyber criminals, such as child predators, producers of child pornography and distributors of child pornography. Ongoing joint investigations by the FBI/DSP HTCU involve other cyber-related violations, including computer intrusions, copyright infringement, wire fraud, and mail fraud.

Street Gangs and Violent Crime

Gangs are no longer limited to urban areas, but have migrated to more rural settings. Gangs have also infiltrated our prisons and even the military. Gangs have diversified from drug running and petty crime to armed robbery, home invasions, mortgage and health care fraud, and even human trafficking.

While local neighborhood gangs pose the most serious crime threat in Delaware, national gangs such as the Bloods, Crips, and Almighty Latin Kings are present and active here. The Delaware Safe Streets Task Force has identified members of the Latin Kings operating in the New Castle County area, including the City of Wilmington. Latin King members are involved in a myriad of criminal activities, including the distribution and sale of narcotics, weapon trafficking, murder, assault, armed robbery, kidnapping, burglary, auto theft, money laundering, extortion, racketeering, public corruption and intimidation and alien smuggling. The gang is also known to order "hits" on correctional officers, rival gang members and members who fail to follow orders.

To combat the threat posed by these dangerous gangs, I have redirected resources to the Delaware Violent Crime Safe Streets Task Force over the past year. This task force is focused on violent gangs, significant crimes of violence, and the apprehension of violent fugitives through sustained, proactive, coordinated investigations of racketeering, drug conspiracy, and firearms offenses.

In the past six months, working with the Wilmington Police Department, we have assigned analysts and Special Agents to provide in-depth assessments of repeat violent criminals and uncover indicators of organized gang activity. These assessments, reviewed by our partners in the Offices of the U.S. Attorney and Delaware Attorney General, will be used by the task force to both target the State's most violent gang members and to determine the most appropriate judicial venue to dismantle these gangs.

It is the FBI's vision that the Delaware Information and Analysis Center (DIAC) - a primary fusion center within the national fusion center network - will become the state's "all source" information repository. Our experience in Maryland has been that the fusion center structure offers the best forum to collect, analyze and disseminate information to the entire law enforcement community. To that end, I am working to staff the DIAC with a full-time analyst under the regular supervision of the Delaware State Police.

Our efforts in this area have already helped the FBI and its partners realize some significant successes. In a recent homicide case, for example, an FBI informant provided valuable information regarding the suspected killers. This information was provided to WPD and resulted in the arrest and conviction of the killer. In another case, an FBI agent working with the DSP to solve an armed robbery case was able to identify a subject from a surveillance photograph as a Latin King. This link enabled the DSP to link other robberies and Latin King members. As I appear before you today, all of the agencies on the Delaware Safe Streets Task Force, including the NCCPD, WPD, DSP, DIAC, FBI, ATF, and DEA, are working to identify active members of the organization for use in ongoing and future investigations.

White Collar Crime

As the home of some of the nation's largest banks and credit card companies, Delaware is an inviting target for white collar criminals. The FBI works closely with local agencies to detect and investigate fraud, theft, or embezzlement occurring within or against Delaware's financial community. In one recent case, the FBI initiated a mortgage fraud investigation based on information provided by the New Castle County Police Department (NCCPD) and the U.S. Marshals. During the course of a parental kidnapping investigation, the NCCPD and Marshals discovered that David Matuisewicz had fraudulently obtained a second mortgage on his home by forging his ex-wife's signature on Wilmington Savings Fund Society (WSFS) documents. Working with the FBI, the NCCPD and Marshals discovered that Matuisewicz had used the proceeds from the mortgage fraud to take his three young daughters out of the U.S. By working together, the FBI, NCCPD, and Marshals located Matusiewicz and the children and traced the money. As a result of this joint effort, the children were returned to their custodial parent and Matusiewicz was sentenced to four years in jail, five years of supervised release and a $9,600 fine. In addition, $250,000 in mortgage fraud proceeds were recovered and returned to WSFS Bank.

The FBI also participates in various working groups dedicated to sharing information on serious financial crimes. For example, the Delaware Mortgage Fraud Working Group reviews and coordinates ongoing investigations, complaints, threats and SARs related to mortgage fraud. Participating agencies include, but are not limited to: FBI, Social Security Administration, IRS,

Delaware Department of Justice (Attorney General's Office), U.S. Housing and Urban Development (HUD OIG), and financial institutions. The FBI also coordinates closely with the Securities and Exchange Commission and the Delaware Attorney General's Office on potential financial frauds. These coordination meetings are critical to assessing and addressing the threat posed by white collar criminals operating in or impacting financial institutions in Delaware.

Drug Trafficking

Drug trafficking is often linked to gang activity and violent crime. The diversion of prescription drugs, such as Oxycodone, is an increasing source of revenue for drug dealers in Delaware and across the nation. The FBI, DEA, and the DSP are sharing information to stem the tide of prescription drugs entering the illegal drug networks in Delaware. In one recent case, the DSP informed the FBI of suspicious money laundering activity by a husband and wife team. Through their joint investigative effort, the FBI, DEA and DSP uncovered a large network of individuals who purchased Oxycodone pills and resold them at a profit to addicts and other drug dealers. As a result of this joint effort, three individuals were arrested on September 12, 2009, and charged with Conspiracy to Distribute Oxycodone and Distribution of Oxycodone. They have since pled guilty and are awaiting sentencing.

Intellectual Property

Intellectual Property Rights (IPR) violations, including theft of trade secrets, digital piracy, and trafficking counterfeit goods, result in billions of dollars of losses each year. These threats also pose significant risk to U.S. public health and safety via counterfeit pharmaceuticals, electrical components, aircraft parts and automobile parts. Protecting intellectual property bolsters confidence in our economy, creates opportunities for growth, and promotes fairness and competitiveness in the marketplace.

IPR investigations are a high priority for the FBI. The FBI is an active partner in, and is co-located at, the National Intellectual Property Rights Coordination Center (IPR Center), an interagency task force consisting of 18 member agencies mandated to combat intellectual property theft. Intellectual property investigations are extremely complicated and difficult to investigate. A criminal organization or hostile intelligence service no longer has to physically infiltrate our businesses or government buildings to steal secrets. With relatively unsophisticated computer hacking skills, terabytes of proprietary information can be downloaded with a few key strokes onto a device smaller than your thumb. U.S. businesses lose billions of dollars, the U.S. government loses critical technology and, oftentimes, these facts are never even known.

A recent example of the FBI's success in this arena in Delaware is the arrest of former DuPont scientist Dr. Hong Meng. Dr. Meng was a synthetic chemist with DuPont who worked to develop Organic Light Emitting Diodes (OLEDs), the future of lighting and display technologies. Unbeknownst to DuPont, Dr. Meng had covertly accepted a position with Peking University as a chemistry professor despite informing DuPont that he planned to transfer to their offices in Shanghai. Dr. Meng emailed trade secret information to his email account at Peking University, solicited investment funding from Chinese provincial governments, and applied for Chinese government grants for OLED-related research. Faced with compelling evidence

collected by the FBI and the U.S. Attorney's Office in Delaware, Dr. Meng pleaded guilty to theft of trade secrets charges in June 2010. He was sentenced to fourteen months in jail and ordered to pay $58,000 in restitution to DuPont.

Conclusion

The FBI remains committed to its responsibility to aggressively combat the threats posed by criminal elements in our communities. To maximize our current resources, we have used our expanded and maturing intelligence collection and analysis capabilities to better identify and understand the growing threat posed by violent criminals. We also continue to rely heavily on the strong relationships we have with our law enforcement and community partners. Much work remains to be done. We will continue to strive for better methods and enhanced communication among partners in law enforcement and the community.

Thank you for allowing me the opportunity to testify before you today. I am happy to answer any questions at this time.