Department of Justice

STATEMENT

OF

ROBERT S. MUELLER, III
DIRECTOR
FEDERAL BUREAU OF INVESTIGATION

BEFORE THE

COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

AT A HEARING ENTITLED

"OVERSIGHT OF THE FEDERAL BUREAU OF INVESTIGATION"

PRESENTED

MARCH 30, 2011

STATEMENT FOR THE RECORD OF
ROBERT S. MUELLER, III
DIRECTOR, FEDERAL BUREAU OF INVESTIGATION
BEFORE THE
COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE
AT A HEARING ENTITLED
"OVERSIGHT OF THE FEDERAL BUREAU OF INVESTIGATION"
PRESENTED
MARCH 30, 2011

I. Introduction

Good morning, Chairman Leahy, Ranking Member Grassley, and Members of the Committee. Thank you for the opportunity to appear before the Committee today.

The FBI has never faced a more complex threat environment than it does today, whether one considers terrorism, espionage, cyber-based attacks, or traditional crimes. Indeed, during the past year, the FBI has faced an extraordinary range of national security and criminal threats.

There were last October's attempted bombings on air cargo flights bound for the United States from Yemen, directed by al Qa'ida in the Arabian Peninsula (AQAP). There was last May's attempted car bombing in Times Square, aided by Tehrik-e-Taliban in Pakistan (TTP). These two attempted attacks demonstrate how al Qa'ida's affiliates and allies have the intent to strike inside the United States.

We have also seen a number of terrorist plots by lone offenders, involving such possible targets as the home of former president George W. Bush; a Christmas-tree lighting ceremony in Portland; and subway stations in the Washington, D.C., Metro system.

There were the arrests last summer of ten Russian spies, known as "illegals," who secretly blended into American society, committed to the long-term goal of clandestinely gathering information for Russia. There was the disclosure of thousands of classified United States diplomatic cables and other documents by WikiLeaks. There was the cyber intrusion at Google as well as countless other cyber incidents that threaten to undermine the integrity of the Internet and to victimize the businesses and people who rely on it.

There were billion-dollar investment and mortgage frauds that undermined the financial system and victimized investors, homeowners, and ultimately taxpayers. There continued to be insidious health care scams involving false billings and fake treatments that endangered patients and fleeced government health care programs.

Continued violence on our Southwest Border led to the murder last March of an American consulate worker, her husband, and the spouse of another Consulate employee in

Juarez, Mexico, as well as the shooting last month of two U.S. Immigration and Customs Enforcement agents in Mexico.

And throughout, there were serious corruption cases that undermined the public trust, and violent gang cases that continued to endanger our communities.

As these examples demonstrate, the FBI's mission to protect the American people has never been broader or more complex, and the demands on the FBI have never been greater.

Since the 9/11 attacks, the FBI has transformed itself into a threat-driven, intelligence-led national security agency whose highest priority is to protect our nation from terrorist attack. But terrorism is by no means our only priority. We have also expanded our capabilities to confront the increased threat of cyber-based attacks, and we continue to maintain our responsibilities for combating public corruption, transnational organized crime, major white-collar crime, and significant violent crimes.

The FBI's transformation is an ongoing effort, and to meet all these challenges in the years to come, we will continue to need the full support of Congress.

II. Counterterrorism

Terrorism, in general, and al Qa'ida and its affiliates, in particular, continue to present the most significant threat to our national security. As we have seen in recent months, al Qa'ida and its affiliates remain committed to conducting attacks inside the United States, and they constantly develop new tactics and techniques to penetrate our security measures.

While the risk posed by core al Qa'ida is clear, organizations such as AQAP and TTP have emerged as significant threats, demonstrating both the intent and capability to attack the homeland as well as our citizens and interests abroad. Take, for example, the attempted 2009 Christmas Day airline bombing, which was directed by AQAP; or last May's failed Times Square car bombing, an attack linked to support from the TTP, a militant group in Pakistan. In each case, these groups were able to recruit individuals committed to attacking the United States, and whose backgrounds were less likely to trigger security scrutiny.

AQAP also took responsibility for directing the attempt last October to send two packages containing plastic explosives and detonators on air cargo flights bound from Yemen to the United States.

We also confront the increasing use of the Internet for spreading extremist propaganda, and for terrorist recruiting, training, and planning. Consider the impact of someone like Anwar Aulaqi – the Yemeni-based extremist. Fifteen years ago, Aulaqi's means of communication were limited. Today, on the Internet, he has unlimited reach to individuals around the world, including those here at home.

In the past ten years, al Qa'ida's online presence has become just as detrimental as its physical presence. As noted above, extremists are not limiting their use of the Internet to

recruitment or radicalization; they are using it to incite terrorism. Thousands of extremist websites promote violence to an online worldwide audience predisposed to the extremist message. They are posting videos on how to build backpack bombs and bio-weapons. They are using social networking to link terrorist plotters and those seeking to carry out these plans

Along with traditional international terrorist groups, homegrown terrorists, as well as domestic terrorist groups, also pose a serious, rapidly evolving threat. There is no typical profile of a homegrown terrorist; their experiences and motivating factors vary widely.

In December, an FBI sting led to the arrest of a 21-year-old man for an alleged plot to bomb a military recruiting center in Catonsville, Maryland. Last November, an FBI sting operation resulted in the arrest of a 19-year-old Somali-American student who allegedly attempted to detonate what he believed was a car bomb during a Christmas-tree lighting ceremony in Portland, Oregon. And last October the FBI arrested a Pakistani-American named Farooque Ahmed, who allegedly plotted to bomb subway stations in the Washington, D.C., Metro system.

The FBI also continues to see the phenomenon of American citizens who become radicalized and then travel overseas to take up arms with terrorist groups. A recent example is Zachary Chesser, a Virginia man arrested last July while attempting to travel to Somalia, where he intended to join the terrorist organization Al Shaabab as a foreign fighter. Last month he received a 25-year prison sentence. Another example is the "D.C. Five," a group of five young American men originally from Northern Virginia who traveled to Pakistan in late 2009. They were sentenced last June in Pakistan to ten years in prison on terrorism-related charges. These cases raise the question whether other such young men will one day return home to the United States, and, if so, what they might undertake here.

Finally, the FBI remains vigilant against the threat of attacks by domestic-based terror groups. In January, a pipe bomb was discovered during a Martin Luther King Day parade in Spokane, Washington. And last March, nine members of the Michigan-based Hutaree Militia were indicted for their alleged involvement in a plot to kill law enforcement officers and possibly civilians using illegal explosives and firearms.

In sum, we are seeing an increase in the sources of terrorism, a wider array of terrorist targets, and an evolution in terrorist tactics and means of communication – all of which makes the FBI's job that much more difficult. These terrorist threats are diverse, far-reaching, and ever-changing. Combating them requires the FBI to continue improving our intelligence and investigative programs, and to continue engaging our intelligence and law enforcement partners, both domestically and overseas. The FBI understands that protecting America requires the cooperation and understanding of the public. Since the 9/11 attacks, the FBI has developed an extensive outreach program to Muslim, South Asian, and Sikh communities to develop trust, address concerns, and dispel myths in those communities about the FBI and the U.S. government. As part of this effort, in 2009 the FBI established the Specialized Community Outreach Team (SCOT), composed of special agents, analysts, community outreach specialists, and personnel with language or other specialized skills. This team assists field offices with establishing new contacts in key communities.

We encourage Congress to reauthorize the three critical FISA tools that will expire later this year: roving wiretap authority, access to business records under FISA and the "lone wolf" provision. Two of these tools have been part of FISA since the USA PATRIOT Act was enacted nearly a decade ago, and the third has been in FISA since 2004. They have all been reauthorized several times. Each facilitates the collection of vital foreign intelligence and counterintelligence information to support our national security mission.

III. Cyber Security

Cyber threats to our national security are broad in nature, from acts of terrorism supported by the use of the Internet, to economic espionage by foreign countries, to sophisticated state-sponsored hackers. Such threats could compromise our national critical infrastructure, from energy, water, telecommunications and transportation systems to financial services.

Cyber Threats

With regard to the terrorist use of the Internet, terrorists have not used the Internet to launch a full-scale cyber attack. But terrorist sympathizers have used the Internet to hide their communications, attempted denial-of-service attacks, and defaced numerous websites. And while the damage may have been limited, such groups may attack for publicity or impact, and they are becoming more adept at both.

The FBI, with our partners in the intelligence community, believes that the threat from the terrorist use of the Internet is a growing terrorist threat area. We speculate they will either train their own recruits or hire outsiders, with an eye toward leveraging physical attacks with use of the internet.

The cyber threat is equally significant with regard to counterintelligence intrusions and economic espionage. Today, our adversaries sit within our networks, often unknown and undetected. They may be nation-state actors or mercenaries for hire, rogue hackers or transnational criminal syndicates.

These hackers actively target both government and corporate networks. They seek our technology and our trade secrets, our intelligence and our intellectual property, even our military weapons and strategies.

The FBI is actively pursuing each of these threats. 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, including the Secret Service, which also has strong capabilities in this area. And they teach their counterparts – both at home and abroad – how best to investigate cyber threats.

But the FBI cannot do it alone. The National Cyber Investigative Joint Task Force includes 20 law enforcement and intelligence agencies, working side by side to share intelligence

and to identify key players and schemes. The goal is to predict and prevent what is on the horizon, and to pursue the enterprises behind these attacks. Last year's takedown of the Mariposa botnet is but one example of that collaboration. As you may know, Mariposa was an information-stealing botnet – one that infected millions of computers, including major banks and other Fortune 1000 companies. And this case, like so many others, emphasized the need for global cooperation. We look forward to working with Congress as it considers whether it should enact legislation requiring companies to report significant breaches of their network security to the FBI and other law enforcement agencies in real time. Such a requirement would promote coordination between appropriate agencies to investigate intrusions, identify the bad actors, and take actions to prevent further damage.

We have more than 60 FBI Legat offices around the world, sharing information and coordinating joint investigations with our host countries. And we have Special Agents embedded with police forces in Romania, Estonia, and the Netherlands, to name just a few. With our partners in the United Kingdom, Germany, and Turkey, we dismantled Darkmarket, one of the most sophisticated online criminal syndicates – and one of the forerunners in using the Internet to buy and sell stolen financial data. We must continue to press forward, country by country, and company by company.

Apart from the national security threat posed by cyber criminals, we confront traditional crime that has migrated and, indeed, flourished, on the Internet, from crimes against children to fraud.

Internet Fraud

With regard to Internet fraud, the 2010 Internet Crime Report was released in February. Last year, the Internet Crime Complaint Center (IC3) received more than 300,000 complaints of Internet crime, the second-highest total in IC3's history. The IC3 is a partnership between the FBI and the National White Collar Crime Center. Since its creation in 2000, IC3 has received more than two million Internet crime complaints.

Last year, IC3 referred more than 120,000 complaints to law enforcement for further investigation. New technology developed for IC3 enables investigators to share information and collaborate on cases that cross jurisdictions, as nearly all cyber crime cases do. IC3 analysts also provide support for investigative efforts.

The IC3 is a unique resource for federal, state, and local law enforcement to intake cases efficiently, find patterns in what might appear to be isolated incidents, combine multiple smaller crime reports into larger, higher priority cases, and ultimately bring cyber criminals to justice.

Innocent Images National Initiative

The Innocent Images National Initiative (IINI), a component of the FBI's Cyber Crime Program, is an intelligence-driven, multi-agency operation combating the proliferation of online child pornography and child exploitation. The mission of the IINI is to reduce the vulnerability of children to acts of sexual exploitation and abuse facilitated through computers; to identify and

rescue child victims; to investigate and prosecute sexual predators who use the Internet to exploit children for personal or financial gain; and to strengthen the capabilities of federal, state, local, and international law enforcement through training and investigative assistance.

From 1996 to 2009, child exploitation investigations in the FBI increased more than 2,500 percent. IINI currently has more than 6,000 child pornography cases. During FY2009 and FY2010, we made more than 2,000 arrests and obtained more than 2,500 convictions. We also identified 246 children exploited in child pornography in FY2010.

The Innocent Images International Task Force brings together law enforcement from around the world to prevent and prosecute online child exploitation. Currently, nearly 100 international officers from 42 countries participate on the task force, which allows for the real-time transfer of information and coordination of cases.

One such investigation, dubbed Operation Achilles, involved our partners in Australia, New Zealand, Canada, Belgium, Italy, and Britain. The three-year investigation uncovered suspects who traded more than 400,000 images of children, many depicting acts of violence and torture. Forty children were rescued, four websites were shut down, and 22 members of the ring were arrested. Fourteen of the 22 members were Americans who were successfully prosecuted by the Justice Department's Child Exploitation and Obscenity Section (Criminal Division) and the U.S. Attorney's Office for the Northern District of Florida.

Crimes Against Children

Child prostitution remains one of our most serious problems. In June 2003, the FBI, the Department of Justice Child Exploitation and Obscenity Section, and the National Center for Missing and Exploited Children joined forces to launch the Innocence Lost National Initiative (ILNI), targeting the growing problem of domestic sex trafficking of children in the United States. Each of the ILNI's 41 task forces and working groups throughout the United States include federal, state and local law enforcement agencies working in tandem with U.S. Attorney's Offices.

The FBI's Crimes Against Children Unit also coordinates an ongoing national sting operation entitled Operation Cross Country to combat domestic sex trafficking of children. ILNI task forces and working groups in 54 cities have participated in the operation by targeting venues such as the street tracks, truck stops, motels, and casinos where children are typically prostituted.

Through Operation Cross Country, more than 2,100 law enforcement officers have joined together to rescue child victims and apprehend those who victimize them. As a result, 248 child victims have been safely recovered during Operation Cross Country, phases I through V, and we have arrested 322 pimps engaged in the commercial sexual exploitation of children. For example, in November 2010, in Operation Cross Country V, the FBI and other agencies recovered 70 children and executed 885 arrests, including 99 pimps.

To date, the ILNI has resulted in more than 600 federal and state convictions and the location and recovery of more than 1,300 children. Together, we have obtained substantial

sentences for those convicted, including six life sentences and numerous others ranging from 25-45 years.

IV. Counterintelligence

The foreign intelligence threat to the United States continues unabated, from traditional means, such as last year's arrest of a network of Russian spies living in the United States, to more contemporary methods of tradecraft. Foreign intelligence services continue to target political and military intelligence, as well as information from economic institutions, both in and outside government. Foreign adversaries, however, do not rely on traditional agent networks alone – they are increasingly making use of non-traditional collectors, such as students, visiting scholars and scientists, and business people.

To counter this threat, the FBI relies on long-standing counterintelligence programs and methods. But we have also developed the National Strategy for Counterintelligence to deter and disrupt more modern counterintelligence threats. Its success relies heavily on strategic partnerships to determine and safeguard those technologies that, if compromised, would result in catastrophic losses to national security. Through our relationships with businesses, academia, and U.S. government agencies, the FBI and its counterintelligence partners can identify and effectively protect projects of great importance to the U.S. government.

With the ongoing WikiLeaks disclosure of classified information, we must also be concerned with insider threat capabilities to gather information for unauthorized disclosure.

The FBI began a review more than a year ago, not related to WikiLeaks events, of information and network access policies through its Information Sharing Policy Board, to better balance policies governing the "need to know" with the "responsibility to share." We wanted to ensure that FBI policy enabled appropriate internal and external sharing, and that statutory and Department of Justice guidance was applied throughout the FBI.

As a result, the FBI has reaffirmed its policy of restricting access to its classified networks and allowing direct access to FBI databases or internal share sites from external networks only when appropriate. We also maintain strict rules governing information sharing to protect the privacy of data related to U.S. persons across the different security and information domains. We have instituted strict enforcement of internal access to restricted data, ensuring information systems and discovery applications use the same access policies.

This past December, as a result of the WikiLeaks investigation, the FBI's Inspection Division began a review of policy compliance within the FBI, especially regarding access to restricted files. The Security Division issued a series of bulletins reminding employees of their responsibility to protect all information, and accelerated deployment of data protection mechanisms, including stricter enforcement of removable media use, the blocking of unauthorized devices, and increased monitoring of data movement throughout the Bureau.

V. Criminal Programs

While national security remains our top priority, criminal programs are a key component of our core mission. And we must recognize that national security is as much about keeping our streets safe from crime as it is about protecting the United States from terrorist attack.

The Uniform Crime Report indicates that crime rates continue to fall in cities across the country. But these numbers may not necessarily reflect what we are seeing on our streets. We confront migrating gang activity, violence and corruption on the Southwest Border, international organized crime, white-collar crime, public corruption, and increasing sophistication in both mortgage fraud and health care fraud.

Financial crime, ranging from mortgage and health care fraud to corporate fraud and public corruption, continues to pose a significant threat to our financial systems. These frauds directly victimize millions of taxpayers, homeowners, shareholders, and everyday citizens alike.

Mortgage Fraud

In FY2010, we had more than 3,000 pending mortgage fraud investigations – compared to roughly 700 cases in 2005. Nearly 70 percent of those investigations exceed losses of more than $1 million each.

The FBI currently has 27 Mortgage Fraud Task Forces and 67 Mortgage Fraud Working Groups nationwide. With representatives of federal, state, and local law enforcement, these teams are strategically placed in mortgage fraud "hot spots" across the country. The FBI also has created the National Mortgage Fraud Team, which oversees the national mortgage fraud program, ensuring that we maximize limited resources, pinpoint the most egregious offenders, and identify emerging trends before they flourish. We must also continue to raise public awareness of mortgage fraud schemes, to better prevent fraud in the first place.

Health Care Fraud

The focus on health care fraud is no less important. The federal government spends hundreds of billions of dollars every year to fund Medicare and other government health care programs, and taxpayers rightly expect these funds to be used to provide health care to senior citizens, children, low-income individuals, and disabled individuals. Most medical professionals, providers, and suppliers work hard to comply with the rules. But too many in the health care industry commit schemes that cheat taxpayers and patients alike, and defraud Medicare and other government programs.

Together with our partners in the Department of Justice and the Department of Health and Human Services, the FBI is fighting back. In FY2010, we recovered a record $4 billion on behalf of taxpayers. This represents an approximate $1.47 billion, or 57 percent, increase over the amount recovered in FY2009, which was itself a record amount. Indeed, over the past three years, we have collectively recovered an average of nearly $7 for every dollar expended. In FY2010, the Department of Justice brought criminal health care fraud charges against 931

defendants, the most ever in a single fiscal year, and we obtained 726 convictions, also a record. And the FBI continues to investigate nearly 2,600 cases of health care fraud.

For example, in February 2011, the Medicare Fraud Strike Force – a partnership between the Department of Justice and the Department of Health and Human Services – charged more than 100 defendants in nine cities, including doctors, nurses, health care companies, and executives, for their alleged participation in Medicare fraud schemes involving more than $225 million in false billing. By all accounts, this stands as the largest federal health care fraud takedown in history.

But these strike forces are only part of the FBI's overall health care fraud efforts. The FBI is the only government investigative entity with jurisdiction over both public and private health care programs, and we are uniquely positioned to investigate a broad spectrum of health care fraud activity. From those who defraud Medicare to individuals committing complex schemes against private insurers such as we saw committed against AFLAC in 2010. Agents and analysts are using intelligence to identify emerging schemes; they are developing new techniques to help mitigate the threat. We are using undercover operations and wiretaps, not only to collect evidence for prosecution, but to cut off the heads of these criminal enterprises so they cannot flourish elsewhere. We have dismantled dozens of criminal enterprises engaged in widespread health care fraud, and we have sought seizures and forfeitures to recover program funds.

Corporate Fraud

The FBI and its law enforcement partners continue to uncover major frauds and Ponzi schemes. At the end of FY2010, the FBI had more than 2,300 active corporate and securities fraud investigations.

In December 2010, President Obama's interagency Financial Fraud Enforcement Task Force (FFETF) announced the results of Operation Broken Trust, which highlighted the prevalence of a wide range of investment fraud schemes around the country during a three-and-a-half month period. This enforcement effort included investigations with hundreds of defendants who committed fraud schemes involving more than 120,000 victims and estimated losses totaling more than $8 billion.

With regard to high-level executive prosecutions, a few notable cases highlight our commitment to finding and convicting those individuals who may have contributed to the recent financial crisis.

In June 2010, Lee Farkas, former chairman of Taylor, Bean, and Whitaker (TBW), a large mortgage origination company, was charged with a $1.9 billion fraud that contributed to the failure of Colonial Bank, one of the largest banks in the United States and the sixth largest bank failure in the country. His trial is scheduled for later this year. On March 2, 2011, Catherine Kissick, a former senior vice president of Colonial Bank and head of its Mortgage Warehouse Lending division, pled guilty to conspiring to commit bank, wire, and securities fraud. She faces a maximum sentence of 30 years in prison. And on February 24, 2011, Desiree

Brown, the former treasurer of TBW, pled guilty to conspiring to commit bank, wire, and securities fraud for her role in this fraud scheme.

On February 25, 2011, Michael McGrath, former President and Owner of U.S. Mortgage Corporation, formerly one of the largest private residential mortgage companies in New Jersey, was sentenced to 14 years in prison for his role in perpetrating a corporate fraud scheme involving the double selling of mortgage loans to Fannie Mae, which resulted in losses in excess of $100 million. And in October 2010, Jeffrey Thompson, former President of Hume Bank, pled guilty to making false statements to the FDIC as part of a bank fraud scheme that caused such significant losses that the bank was pushed into insolvency. Thompson faces a sentence of up to 30 years in federal prison without parole, plus a fine up to $1 million and an order of restitution.

These are just a few examples of the thousands of financial fraud investigations ongoing at the FBI and conducted in conjunction with the administration's Financial Fraud Enforcement Task Force.

Public Corruption

The FBI recognizes that fighting public corruption is vital to preserving our democracy, protecting our borders, and securing our communities. Indeed, public corruption remains our top criminal priority.

On October 10, 2010, 89 law enforcement officers and 44 others were arrested and charged in Puerto Rico as part of Operation Guard Shack, the largest police corruption investigation in the history of the FBI. Close to 750 FBI agents were flown in to Puerto Rico from across the country to assist in the arrests. This two-year multi-jurisdictional, multi-agency operation sent a powerful message – that corruption among our public officials will not be tolerated.

The FBI is also working to confront international contract corruption. The FBI's Criminal Investigative Division joined with our federal law enforcement partners to stand up the International Contract Corruption Task Force (ICCTF), which includes all fraud against the U.S. government where the illegal conduct occurred outside the United States and involves United States persons or funds. Since 2004, the ICCTF has initiated nearly 800 investigations in Afghanistan, Iraq, and Kuwait.

For example, in December 2009, Major John Lee Cockerham, Jr., a former U.S. Army contracting officer, was sentenced to more than 17 years for his participation in a bribery and money-laundering scheme related to bribes paid for contracts awarded in support of the Iraq war. Cockerham was convicted of receiving favors, cash, and items of value from contractors in exchange for favorable treatment and consideration on contracts awarded in Iraq and Kuwait. Once he agreed to take money in exchange for awarding contracts, Cockerham directed the contractors to pay his wife, sister, and others to hide the fact that contractors were paying bribes. His wife has since been sentenced to 41 months in prison. His sister received 70 months for her role in the scheme. The total restitution orders included more than $14 million.

As Assistant Attorney General Lanny Breuer noted in his January 2011 testimony before the Senate Judiciary Committee, the Department of Justice and the FBI is also steadfastly pursuing corporate corruption and bribery in violation of the Foreign Corrupt Practices Act ("FCPA"). This corruption and bribery works to the detriment of us all, undermining the transparency and honesty of corporate culture. In 2010, we recovered over $1 billion through resolutions of FCPA investigations, more than in any other year in the history of our FCPA enforcement efforts.

Gang Violence

Every day, violent gangs infiltrate new neighborhoods, new schools, and new street corners. Gangs are no longer limited to urban areas, but have migrated to more rural settings, from Billings, Montana, and Salt Lake City, Utah, to Charlotte, North Carolina, and Omaha, Nebraska. 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, even human trafficking. The economic impact of their criminal activity is estimated to be $5 billion each year.

We have over 230 Violent Gang, Safe Streets, and Safe Trails Task Forces across the country. Through these task forces, we identify and target major groups operating as criminal enterprises. Much of our intelligence comes from our state and local law enforcement partners, who know their communities inside and out. We are using enhanced surveillance and embedded sources to track these gangs, and to identify emerging trends. In the past six months, we have arrested more than 3,500 gang members. To date, we have obtained more than 1,400 convictions. And we have recovered roughly $19 million in forfeitures and seizures. Additionally, the FBI is a strong participant in GangTECC, a DOJ multiagency gang coordination initiative.

By conducting these multi-subject and multi-jurisdictional investigations, the FBI can concentrate on high-level groups engaged in patterns of racketeering. This investigative model enables us to target senior gang leadership and to develop enterprise-based prosecutions.

Organized Crime

We are also concerned with the increased presence and impact of international organized criminal enterprises. Some believe that organized crime is a thing of the past. Unfortunately, this is not the case. Traditional criminal syndicates still con, extort, and intimidate American citizens. On January 20, 2011, we arrested nearly 130 members of La Cosa Nostra in New York, New Jersey, and New England. And we will continue to work with our state and local partners to end La Cosa Nostra's lifelong practice of crime and undue influence.

But we have seen a shift from regional families with clear structures to flat, fluid networks with global reach. These international enterprises are running multi-national, multi-billion dollar schemes from start to finish. In an October 13, 2010, health care fraud takedown, 73 members and associates of organized crime groups (for example, Mirzoyan-Terdjanian Organization) were among those indicted for more than $163 million in health care fraud

crimes. Among the defendants charged is Armen Kazarian, who is alleged to be a "Vory-V-Zakone," a term translated as "Thief-in-Law" and referring to a member of a select group of high-level criminals from Russia and the countries previously part of the former Soviet Union, including Armenia.

On September 16, 2010, 44 members of a Chinese/Korean criminal enterprise involved in a highly sophisticated fraudulent document and identity theft operation were arrested in New Jersey and New York. The charges included aggravated identity theft, passport fraud, bank fraud and tax evasion. The investigation was spawned by a Chicago investigation, which resulted in arrests of 30 members of an Asian criminal enterprises involved in the manufacture and distribution of "identity sets." Each identity set consists of an altered People's Republic of China passport and an authentic SSN. DHS estimates the actual damage inflicted by the "586" fraud network to be in the vicinity of $400 to 500 million since mid-2006, reflecting a significant economic impact on citizens and financial institutions in the United States.

We are also taking a hard look at other groups around the world, including West African and Southeast Asian organized crime. We are sharing that intelligence with our partners who, in turn, will add their own information. The goal is to combine our resources and our expertise to gain a full understanding of each group, and to better understand what we must do, together, to put them out of business. The FBI is also contributing to this end through its participation in the International Organized Crime Intelligence Operations Center (IOC).

Violence and Corruption Along the Southwest Border

The U.S. border with Mexico extends nearly 2,000 miles, from San Diego, California, to Brownsville, Texas. At too many points along the way, drug cartels transport kilos of cocaine, methamphetamine, heroin, and marijuana, gangs kidnap and murder innocent civilians, traffickers smuggle human cargo, and corrupt public officials line their pockets by looking the other way – any one of these offenses represents a challenge for law enforcement. The severity of this problem is highlighted by the following statistics:

- Between 18 and 39 billion dollars flow annually from the United States across the Southwest Border to enrich the Mexican drug cartels.

- Over 3,000 drug-related murders in Juarez, Mexico, in 2010.

- Over 34,600 drug-related murders in all of Mexico from December 2006 to December 2010.

- Estimated that 95 percent of all South American cocaine that moves from South America to the United States goes through Mexico.

- 701,000 kilograms of marijuana were seized during the first five months of 2010 in Arizona, California, New Mexico, and Texas.

To address corruption on the Southwest border, we have 13 border corruption task forces with roughly 120 agents in FBI field offices in the region, and one National Border Corruption Task Force at FBI Headquarters to direct these efforts. We have border liaison officers who work one-on-one with their law enforcement counterparts in Mexico.

To address security along the Southwest Border, we have developed an intelligence-led, cross-programmatic strategy to penetrate, disrupt and dismantle the most dangerous organizations and bring top criminals to justice. This strategy begins with the deployment of hybrid squads in hot spots throughout the area, from Albuquerque, El Paso, and San Antonio, to Dallas, Phoenix, and San Diego.

The goal of the hybrid squad model is to bring expertise from multiple criminal programs into these dynamic, multi-faceted threats and then target, disrupt, and dismantle these organizations. Hybrid squads consist of multi-disciplinary teams of Special Agents, Intelligence Analysts, Staff Operations Specialists, and other professionals. The agent composition on the squads provides different backgrounds and functional expertise, ranging from gang activity and violent crime to public corruption.

Our first success with these hybrid squads came in July 2010, with Operation Luz Verde, which resulted in the arrest of 43 individuals affiliated with the Arellano Felix drug trafficking organization, including a high-ranking official in the Baja Attorney General's Office.

The recent focus on Barrio Azteca, one of the narcotics-focused gangs responsible for the violence in cities like Juarez, Mexico, illustrates this approach. Barrio Azteca has been tied to drug trafficking, prostitution, extortion, assaults, murder, and the retail sale of drugs. Most recently, the gang was linked to the murder of a U.S. Consulate employee, her husband, and the spouse of another Consulate employee in Juarez.

The FBI has been working closely with DHS in a joint effort to investigate the attack against two ICE special agents in Mexico on February 15, 2011, by suspected members of a Mexican drug trafficking organization. Jaime Zapata and Victor Avila were ambushed while traveling from Matehuala, Mexico, to Mexico City in an armored vehicle with diplomatic license plates. Agent Zapata was killed in the attack. The Department of Justice created a joint task force to investigate these shootings, with the FBI as the lead task force agency. On February 24, 2011, Mexican law enforcement detained six individuals in connection with the shooting.

Indian Country

The FBI has the primary federal law enforcement authority for felony crimes in Indian Country. Even with demands from other threats, Indian Country law enforcement remains a priority for the FBI. Last year, the FBI handled more than 2,400 Indian Country investigations throughout the country.

Approximately 75 percent of all FBI Indian Country investigations involve homicide, crimes against children, or felony assaults. Available statistics indicate that American Indians and Alaska Natives suffer violent crime at far greater rates than other Americans. Violence

against Native women and children is a particular problem, with some counties facing murder rates against Native women well over 10 times the national average.[1] In addition to violence, there is a significant emerging threat from fraud and other white-collar crimes committed against tribally run gaming facilities.

Currently, the FBI has 18 Safe Trails Task Forces focused on drugs, gangs and violent crimes in Indian Country. The gang threat on Indian reservations has become evident to the tribal community leaders, and gang related violent crime is reported to be increasing. Tribal community leaders have reported that some youth are bringing back gang ideology from major cities, and Drug Trafficking Organizations are recruiting tribal members.

The FBI's Indian Country Special Crimes Unit works with the Bureau of Indian Affairs Office of Justice Services to sponsor and promote core training for investigators. The FBI provides training for state, local, tribal, and federal investigators regarding gang assessment, crime scene processing, child abuse investigations, forensic interviewing of children, homicide investigations, interviewing and interrogation, and Indian gaming. Furthermore, the FBI's Office of Victim Assistance dedicates a significant number of Victim Specialists to Indian Country to assist the victims of these crimes.

Information Technology

The FBI continues to improve how we collect, analyze, and share information using technology. Intelligence provides the information we need, but technology further enables us to find the patterns and connections in that intelligence. Through sophisticated, searchable databases, we are working to track down known and suspected terrorists through biographical information, travel histories and financial records. We then share that information with those who need it, when they need it.

Earlier this month, the FBI's Criminal Justice Information Services division started using the Next Generation Identification (NGI) System – new technology that will enhance our ability to more quickly and efficiently identify criminals and terrorists, here at home and around the world. With NGI, we are incrementally replacing the Integrated Automated Fingerprint Identification System, which provides automated fingerprint and latent search capabilities to more than 18,000 law enforcement and criminal justice partners, 24 hours a day, 365 days a year. With this new technology, we will have the ability to process fingerprint transactions much faster and with more accuracy.

We are also working to better integrate data sets throughout the Bureau. For example, the FBI has developed the Data Integration and Visualization System (DIVS), with the goal to prioritize and more effectively integrate nearly 200 datasets across the Bureau. The FBI currently has investigative data that is stored and accessed in multiple systems. As a consequence, our personnel are spending too much time hunting for data, leaving them less time to analyze that data to stay ahead of threats.

[1] Zaykowki, Kallmyer, Poteyeva & Lanier (Aug. 2008), *Violence Against American Indian and Alaska Native Women and the Criminal Justice Response: What is Known*, Bachman (NCJ # 223691), at 5, http://www.ncjrs.gov/pdffiles1/nij/grants.223691.pdf.

DIVS provides single sign-on, role-based access controls to analyze and link all FBI data that the user is lawfully allowed to see and will provide the means to efficiently feed FBI Secret data to the FBI Top Secret system. DIVS will not only significantly improve users' efficiency in searching multiple databases, it will ultimately help reduce or eliminate redundant data systems.

Finally, I would like to touch on the Sentinel program. The first two phases of the Sentinel case management system have been deployed and are used by thousands of agents, analysts, and supervisors to access, retrieve, and manage information necessary for FBI operations. The FBI is using agile software development processes to build on the existing program and complete the additional capabilities and functionality of Sentinel.

The Sentinel development team is working in two-week sprints to finish the project. Every two weeks, new capabilities are demonstrated to the FBI's senior executives, with formal monthly updates to the Department of Justice. These smaller development teams provide more flexibility in prioritizing our requirements, incorporating user feedback more quickly and meeting our goals, step by step. The next significant functions are scheduled to be in place in April 2011, with Sentinel scheduled to be operational in September 2011.

One lesson we have learned in recent years is the need to ensure that as new technology is introduced into the marketplace, the FBI and its law enforcement partners maintain the technical capabilities to keep pace. In the ever-changing world of modern communications technologies, however, the FBI and other government agencies are facing a potentially widening gap between our legal authority to intercept electronic communications pursuant to a court order and our practical ability to actually intercept those communications.

As the gap between authority and capabilities widens, the Federal government is increasingly unable to collect valuable evidence in cases ranging from child exploitation and pornography to organized crime and drug trafficking to terrorism and espionage – evidence that a court has authorized us to collect. We need to ensure that our capability to execute lawful court orders to intercept communications does not diminish as the volume and complexity of communications technologies expand.

Similarly, our investigations can be stymied by the records preservations practices of private communications providers. Current law does not require telephone companies and Internet service providers to retain customer subscriber information and source and destination data for any set period of time. This has resulted in an absence of data that may hinder crucial evidence in a child exploitation cases, terrorism, online piracy, computer hacking, and other privacy-related crimes, for example. We look forward to continuing to work with Congress as it considers whether legal changes are needed, and to ensure that any such changes are narrowly tailored to provide targeted government access to information consistent with the protection of privacy and civil liberties.

Conclusion

I appreciate the opportunity to review some of the FBI's recent work responding to the complex and far-ranging threats we face today. I also want to thank the Committee for your continued support of the FBI's mission, which has been essential to our ability to meet these diverse challenges. We will continue to need your support to complete the Bureau's transformation and to meet the full responsibilities of our mission.

I look forward to working with the Committee during the remainder of my tenure as Director to improve the FBI and strengthen its ability to keep the nation safe. I would be happy to answer any questions that you may have.