



# Department of Justice

---

STATEMENT OF

ROBERT S. MUELLER, III  
DIRECTOR  
FEDERAL BUREAU OF INVESTIGATION  
UNITED STATES DEPARTMENT OF JUSTICE

BEFORE THE

UNITED STATES HOUSE OF REPRESENTATIVES  
COMMITTEE ON THE JUDICIARY

HEARING ENTITLED

“THE FEDERAL BUREAU OF INVESTIGATION”

PRESENTED

May 20, 2009

## **I. Introduction**

Good morning Chairman Conyers, Ranking Member Smith, and Members of the Committee. I am pleased to be here today.

As you know, we in the Federal Bureau of Investigation (FBI) have undergone unprecedented transformation in recent years, from developing the intelligence capabilities necessary to address emerging terrorist and criminal threats, to creating the administrative and technological structure necessary to meet our new mission as a national security service.

Today, the FBI is a stronger organization, combining greater intelligence capabilities with a longstanding commitment to protecting the American people from criminal threats. We are also mindful that our mission is not just to safeguard American lives, but also to safeguard American liberties.

I want to give you a brief sense of the FBI's current priorities, the key changes we have made in recent months, and the challenges we face.

## **II. FBI Transformation**

In the aftermath of the September 11, 2001, attacks, counterterrorism became our top priority, and it remains our top priority today. Indeed, our top three priorities – counterterrorism, counterintelligence, and cyber security – are national security related. As a result of that shift in our mission, we have made a number of changes in the FBI, both in structure and in the way we do business.

## **A. Restructuring of FBI Intelligence Program**

We have expanded our counterterrorism operations, strengthened our capacity to collect, analyze and use intelligence on potential threats, and expanded our partnerships with other intelligence agencies.

Inside the FBI, we stood up the National Security Branch and the Weapons of Mass Destruction Directorate. We hired hundreds of intelligence analysts, linguists, and surveillance specialists. We created Field Intelligence Groups (FIGs) in each of our 56 field offices. And, we are conducting a strategic, nationwide re-organization of the FBI that has already improved our ability to identify, evaluate and prevent attacks before they get off the ground.

These changes are part of our ongoing campaign to “Know Our Domain,” as we say. Domain awareness is a 360-degree understanding of all national security and criminal threats in any given city or community. It is the aggregation of intelligence, to include what we already know and what we need to know, and the development of collection plans to find the best means to answer the unknowns. It involves intelligence analysts and special agents gathering, analyzing, and using information about threats, and sharing it in near real-time within a community, across the country, and around the world. With this knowledge, we can allocate resources effectively, identify and neutralize emerging threats, and develop new opportunities for intelligence collection and criminal prosecution.

Here are a few examples of the changes we’ve made in order to maximize the effectiveness of our intelligence program and realize our goal to “Know Our Domain.”

We established a Strategic Execution Team (SET) to help us assess our intelligence program, and to standardize it throughout the FBI. The SET, made up of agents and analysts, developed a series of recommendations for accelerating the integration of our intelligence and investigative work. The SET improvements will ensure that we capitalize on our intelligence collection capabilities and develop a national collection plan to fill gaps in our knowledge base. Our objective is to defeat national security and criminal threats by operating as a single intelligence-led operation, with no dividing line between our criminal and counterterrorism programs. We want to make sure that nothing falls through the cracks.

To this end, we have restructured the FIGs in every field office across the country. FIGs are designed to function as the hub of the FBI's intelligence program. They ensure that each field office is able to identify, assess, and attack emerging threats before they flourish. Following the SET's recommendations, the FIGs now conform to one model, based on best practices from the field, and adapted to the size and complexity of each office. Each FIG has well-defined requirements for intelligence gathering, analysis, use, and production. Managers are accountable for ensuring that intelligence production is of high quality and relevant not only to their own communities, but to the larger intelligence and law enforcement communities.

As a result of these changes, the analysts and agents in the FIGs collect intelligence more completely, analyze it more quickly, share it more widely with others who need the information, and take action on it more effectively. Now, FIGS can better coordinate with each other and with Headquarters. And, they can better coordinate with law enforcement and intelligence partners, and the communities they serve. With this

integrated model, we can turn information and intelligence into knowledge and action, from coast to coast.

We are now in the process of implementing SET concepts at FBI headquarters, to improve strategic alignment between the operational divisions and the Directorate of Intelligence. We want to better manage national collection requirements and plans, and ensure that intelligence from our Field Offices is integrated and shared with those who need it at FBI headquarters and in the larger Intelligence Community.

This is not a program that will be implemented as a quick fix. The work of the SET is critical to the long-term success of the FBI. We are training FBI personnel at all levels in order to help us execute these plans long past the initial rollout. We have clear metrics for success, and clear lines of accountability to ensure that we reach our goals. We are committed to implementing these plans and making our national security and intelligence capabilities even stronger.

In addition to our work inside of the FBI, we integrated our intelligence program with other agencies under the Director of National Intelligence, with appropriate protections for privacy and civil liberties. And, we participate in, and share information with, multi-agency intelligence centers, including the Organized Crime Drug Enforcement Task Forces Fusion Center, the El Paso Intelligence Center, and the National Drug Intelligence Center. In short, we have improved our national security capabilities across the board.

## **B. Improvements to FBI Technology**

I want to turn for a moment to recent improvements in FBI technology. We cannot gather the intelligence we need, analyze that intelligence, or share it with our law enforcement or intelligence partners, without the right technology. The right technology will also be crucial to protecting privacy interests and ensuring proper use of sensitive information.

One of our most important programs is Sentinel, our web-based case management system. Phase I was deployed FBI-wide in June 2007. Information is now pushed to users electronically, moving employees away from dependence on paper files and making it faster and easier to access and connect information.

Phase I set the foundation for the entire enterprise. We are working with Lockheed Martin to implement Phase II in increments, with a target completion date of Fall 2009. Throughout this phase, we are delivering new capability to all users with the migration of full Administrative Case Management to Sentinel. Phases III and IV are scheduled to be delivered in early Spring 2010 and Summer 2010, respectively.

Proper training will be provided to all users, ensuring maximum exploitation of Sentinel's capabilities.

We are also strengthening the information technology (IT) programs that allow us to communicate and share with our partners. For example, we launched an initiative to consolidate the FBI's Unclassified Network with Law Enforcement Online (LEO), which is the unclassified secure network we use to share information with registered law enforcement partners.

This will provide a single platform that allows FBI employees to communicate and share with their internal and external partners. Currently, LEO provides a secure communications link to and among all levels of law enforcement and is available to more than 18,000 law enforcement agencies. LEO has a user community of more than 137,000 vetted members.

As part of the LEO platform, the FBI is delivering the eGuardian system – an unclassified counterterrorism tool available to our federal, state, local, and tribal law enforcement partners through the FBI’s secure LEO internet portal. The eGuardian system will work in tandem with Guardian, the FBI’s classified web-based counterterrorism incident management application. Guardian makes threat and suspicious activity information immediately available to all authorized users. Guardian will then make available unclassified threat and suspicious activity information through eGuardian, enabling law enforcement personnel to receive the most current information. In return, any potential terrorist threat or suspicious activity information provided by law enforcement will be made available in Guardian entries and outward to the FBI task forces.

In September 2008, we piloted eGuardian to several fusion centers, the Department of Defense, and the Federal Air Marshal Service. Today, eGuardian has been deployed nationwide to enable near real-time information sharing and tracking of terrorist information and suspicious activities with the FBI’s federal, State, local, and tribal partners.

We are also in the midst of developing what we call “Next Generation Identification” system, which enhances the FBI’s fingerprint-based identification, known

as the Integrated Automated Fingerprint Identification System, to include better ways to exchange biometric data. This will better enable us to find criminals and terrorists who are using the latest technology to shield their identities and activities. In support of our multi-modal biometrics efforts, we have also established the Biometrics Center of Excellence at our Criminal Justice Information Services (CJIS) complex in West Virginia. Its mission is to serve as a research and development, test and evaluation, and standards promulgation center for not only U.S. law enforcement, but for other government entities that share similar challenges in the positive identification of individuals of concern.

We have also developed a system called the Law Enforcement National Data Exchange, (N-DEx). N-DEx is a national information-sharing system, accessible to law enforcement agencies through a secure website. It will allow nationwide searches from a single access point and leverages the current IT infrastructure managed by our CJIS division that already interconnects almost every US law enforcement agency. We successfully completed the initial deployment last year and will continue to refine and expand it.

Through N-DEx, law enforcement officers will now be able to search databases for information on everything from tattoos to cars, allowing them to link cases that previously seemed isolated. They will be able to see crime trends and hotspots, access threat level assessments of individuals or locations, and make the best use of mapping technology. It is not a new records management system, but one that allows us to share and link the information we already have.



The FBI also participates in OneDOJ. The OneDOJ System is the result of the Department of Justice Law Enforcement Information Sharing Program strategy among the FBI, Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF), Bureau of Prisons, Drug Enforcement Administration (DEA), and the United States Marshals Service, for the exchange of investigative case/incident, arrest, booking, and incarceration data. These agencies are considered Department of Justice (DOJ) component users, while regional sharing systems are considered remote local, state, and federal law enforcement partners. OneDOJ supports the DOJ component users and remote law enforcement investigators and analysts through storage for contributed data, services for structured and unstructured searching of remote partner data stores and DOJ data, notification, secure communications, and reporting. Currently, the FBI's Criminal Justice Services Division is tightly integrating the OneDOJ System into the Law Enforcement National Data Exchange System for national level investigative information sharing.

We are also working to improve our confidential human source management system. Intelligence provided by confidential human sources is fundamental to the FBI mission. To better manage that data, we are putting in place a program known as DELTA. DELTA will provide FBI agents and intelligence analysts a uniform means of handling the administrative aspect of maintaining human sources. It will also enable FBI headquarters and field offices to better understand, connect, operate, and protect confidential human sources.

We are also improving our crisis management systems. The Operational Response and Investigative Online Network (ORION) is the FBI's next-generation Crisis Information Management System, which provides crisis management services to federal,

state, local, and tribal law enforcement and/or emergency personnel. ORION standardizes crisis and event management processes, enhances situational awareness, and supports the exchange of information with other command posts.

ORION provides a web-based crisis management application hosted on the Sensitive But Unclassified and FBI Secret networks that is also deployable in a stand-alone configuration via Critical Incident Response Group Fly-kits to locations without Internet or Secret network access. The ORION application is accessible from almost any desktop with FBINET or UNET connectivity using a standard web browser. It has been used at both the Democratic and Republican national conventions, major sporting events, to include the Olympics, and this year's Inauguration.

I know the FBI's progress in reducing the backlog of name check requests, especially in the area of immigration, has been of great interest to Members of Congress. We have made significant improvement during Fiscal Year (FY) 2008, with that trend continuing into FY 2009. At the beginning of FY 2008, the FBI had over 402,000 pending name check requests submitted by the United States Citizenship and Immigration Services (USCIS), with over 380,000 of those pending for more than 30 days. As of March 31, 2009, the FBI has processed over 99 percent of all incoming USCIS name checks within 60 days for the fiscal year and had only 30 USCIS name check requests pending for more than 30 days. The FBI will build on this success and will further streamline and improve the name check process.

### **C. Human Capital**

These improvements in structure and technology will strengthen the FBI's intelligence capabilities. But we know that people are the FBI's best and strongest asset – one we must capitalize on to achieve our mission.

As you know, we have been hard at work building a strong Human Resources program to ensure we have the optimum recruiting, hiring, training, and retention practices for our employees.

The changing workforce of the United States will have different expectations than previous generations, challenging the FBI to evolve its career development practices and offer new opportunities for growth in order to attract talent. We must also continue to enhance our intelligence capabilities, adding to the skill sets of on-board employees. Finally, we must ensure there is sufficient leadership bench strength to lead the organization now and into the future.

Historically, the FBI has attracted recruits from the law enforcement, legal, and military communities, particularly to fill our Special Agent ranks. This has served us well as a law enforcement agency.

But as we develop into a national security agency, we also require employees with specialized skills — intelligence analysts, surveillance specialists, scientists, linguists, and computer experts.

Our hiring for FY 2009 includes goals to bring on board approximately 2,800 professional staff, including intelligence analysts, information technology specialists, language specialists, and 850 new agents. Through our recruiting efforts, we have received more than 450,000 applications. We have extended more than 5,500 job offers

and continue to work through the tremendous response from Americans who want to dedicate their careers to public service.

In order to help our people achieve their career aspirations, we have created career paths for agents and analysts alike. For example, the intelligence analyst career path provides early training, including a developmental rotational program, mentoring, and a range of job experiences, as well as opportunities for advancement. We have also developed a dedicated career path for Special Agents who specialize in intelligence. Our goal is to establish career paths for all employees.

We are also focused on strengthening our training programs. The FBI Academy at Quantico and the National Academy have long been considered premier law enforcement training academies. We are enhancing our Intelligence Training School at Quantico to build similarly strong intelligence skill sets. We are leveraging our Intelligence Community partners to help us develop curriculum and provide expert instruction, including a recently introduced human intelligence training course that we developed jointly with the Central Intelligence Agency.

A 2009 priority is to revamp our approach to developing leaders at all levels of the FBI. To that end, we have launched a leadership development initiative to identify and implement an interconnected set of leadership training and developmental experiences for all employees, at all levels.

In order to support our human resources programs, we have also launched an initiative to transition the FBI to an updated Human Resources Information System. We are evaluating systems to identify the best platform for the FBI, which will provide us

with the technological infrastructure that managing a strong Human Resources program requires.

Diversity in the FBI workforce is one of my top human resource priorities. Improving the diversity of our workforce at every level of the organization requires a top-to-bottom effort to recruit, train, retain and promote qualified women, minorities, and persons with disabilities. For example, for some time now, we have been recruiting aggressively in historically black colleges, through the association of Hispanic colleges, and at tribal universities. We have also been placing targeted ads in minority-oriented radio programs, periodicals, job fairs, and other venues that are designed to reach minority communities. We have made progress in our efforts to diversify the FBI, but much work remains to be done.

We are committed to investing the time and resources to provide the training and development, mentoring, and job experiences that will hone our employees' management, leadership, and technical skills. Today's new employees are the leaders of tomorrow's FBI, and we are committed to ensuring the FBI has continuous and strong leadership well into the future.

### **III. Threat Overview**

These improvements are necessary for the work ahead of us. The threats we face are diverse, dangerous, and global in nature.

## **A. Counterterrorism**

As you know, terrorism remains our top priority. We have not had a terrorist attack on American soil in more than seven years, but that by no means indicates the threat is over. We must continue to be vigilant.

Today, we still face threats from Al Qaeda. But we must also focus on less well-known terrorist groups, as well as homegrown terrorists. And we must consider extremists from visa-waiver countries, who are merely an e-ticket away from the United States. Our primary threat continues to come from the tribal areas of Pakistan and Afghanistan. But we are seeing persistent activity elsewhere, from the Horn of Africa to Yemen.

We are also concerned about the threat of homegrown terrorists. Over the years since September 11, 2001, we have learned of young men from communities in the United States, radicalized and recruited here to travel to countries such as Afghanistan or Iraq, Yemen or Somalia. We must also focus on extremists who may be living here in the United States, in the very communities they intend to attack.

Given these substantial threats, terrorism will remain our top priority. But it is by no means our only priority.

## **B. Economic Crime**

In the wake of September 11<sup>th</sup>, we were confronted with radical changes to the FBI – changes that were necessary to address the terrorist threat. Yet at the same time, we faced a rash of corporate wrongdoing, from Enron and WorldCom to Qwest. We needed to prioritize our resources.

Public corruption is our top criminal priority. We have approximately 2,500 pending public corruption investigations and have seen a significant increase in public corruption cases since 2003. In the past five years, the number of agents working public corruption cases has consistently increased to the current level of over 600 agents. And we have convicted more than 1,618 federal, state, and local officials in the past two years alone.

Apart from public corruption, economic crime remains one of our primary concerns. Our mortgage fraud caseload has more than tripled in the past three years, from over 800 cases to more than 2,400. In addition, the FBI has more than 560 open corporate fraud investigations, including matters directly related to the current financial crisis.

To meet this challenge, we have had to re-prioritize our criminal programs to address the current financial crisis. In FY 2007, we had 120 agents investigating mortgage fraud cases. In FY 2008, that number increased to 180 agents, and currently over 260 agents are assigned to mortgage fraud and related cases.

Unfortunately, there is no sign that our mortgage fraud caseload will decrease in the near future. To the contrary, Suspicious Activity Reports (SARs) from financial institutions have indicated a significant increase in mortgage fraud reporting filed with the Financial Crimes Enforcement Network (FinCEN). For example, during FY 2008, mortgage fraud SARs increased more than 36 percent to a total of 63,173. So far in FY 2009, there have been 33,291 mortgage fraud SARs filed. While the total dollar loss attributed to mortgage fraud is unknown, seven percent of SARs filed in FY 2008 indicated a specific dollar loss, which totaled more than \$1.5 billion.

To make the best use of our resources, the FBI has found new ways to detect and combat mortgage fraud. One example is the use of a property flipping analytical computer application, first developed by the Washington Field Office, to effectively identify property flipping in the Baltimore and Washington areas.

This original concept has evolved into a national FBI initiative that employs statistical correlations and other advanced computer technology to search for companies and persons with patterns of property flipping. As potential targets are analyzed and flagged, information is provided to the respective FBI Field Office for further investigation.

In addition, sophisticated investigative techniques, such as undercover operations and wiretaps, not only result in the collection of valuable evidence, they provide an opportunity to apprehend criminals in the commission of their crimes, thus reducing loss to individuals and financial institutions. By pursuing these proactive methods in conjunction with historical investigations, the FBI is able to realize operational efficiencies in large scale investigations.

In December 2008, the FBI dedicated resources to create the National Mortgage Fraud Team at FBI headquarters. The team has specific responsibility for the management of the mortgage fraud program at both the origination and corporate level. They will assist FBI field offices in addressing the mortgage fraud problem at all levels. And they will provide tools to identify the most egregious mortgage fraud perpetrators, prioritize pending investigations, and provide information to evaluate where additional manpower is needed.



One of the best tools the FBI has for combating mortgage fraud is its long-standing partnerships with government and industry partners. Currently, there are 18 mortgage fraud task forces and 50 working groups across the country. These task forces are strategically placed in areas identified as high threat areas for mortgage fraud.

Partners are varied, but typically include representatives of Housing and Urban Development, the U.S. Postal Inspection Service, the Internal Revenue Service, Financial Crimes Enforcement Network, the Federal Deposit Insurance Corporation, and State and local law enforcement officers. This multi-agency model serves as a force multiplier, providing an array of resources to identify the source of the fraud and finding the most effective way to prosecute each case.

Last June, for example, we worked closely with our partners on “Operation Malicious Mortgage”, a multi-agency takedown on mortgage fraud schemes, with more than 400 defendants across the country. Thus far, 164 defendants have been convicted in federal, State, and local courts for crimes that amount to more than \$1 billion in losses. Forty six of our 56 field offices took part in the operation, which has also resulted in the forfeiture or seizure of more than \$60 million in assets.

The FBI is one of the DOJ participants in the national Mortgage Fraud Working Group, which DOJ chairs. Together, we are building on existing FBI intelligence databases to identify large industry insiders and criminal enterprises conducting systemic mortgage fraud.

We also continue to foster relationships with representatives of the mortgage industry to promote mortgage fraud awareness. We are working with industry partners to develop a more efficient mortgage fraud reporting mechanism for those not mandated to

report such activity. This Suspicious Mortgage Fraud Activity Report concept is being discussed with FinCEN and is under consideration by the Mortgage Bankers Association.

The FBI is the primary federal investigative agency involved in the fight against health care fraud. National health care spending in the United States exceeded \$2.2 trillion and represented 16 percent of the Nation's Gross Domestic Product in 2007. The Federal Government financed more than one-third of the Nation's health care that year; federal and state governments collectively financed 46 percent of U.S. health care costs. The National Health Care Anti-Fraud Association estimates that 3 percent of the nation's health care spending—or more than \$60 billion each year—is lost to fraud. With health care expenditures rising at three times the rate of inflation, it is especially important to coordinate all investigative efforts to combat fraud within the health care system. More than \$1 trillion is spent in the private sector on health care and its related services and the FBI's efforts are crucial to the overall success of the program. The FBI leverages its resources in both the private and public arenas through investigative partnerships with agencies such as the Department of Health and Human Services Office of the Inspector General, the Food and Drug Administration, the DEA, the Defense Criminal Investigative Service, the Office of Personnel Management, the Internal Revenue Service, and various state and local agencies. The FBI is actively involved with national groups, such as the National Health Care Anti-Fraud Association, the Blue Cross and Blue Shield Association, the National Insurance Crime Bureau, and many other agencies, organizations, and professional associations in an effort to expose and investigate fraud within the system.

The Department of Justice and the FBI have resources in every region of the country to investigate and prosecute health care fraud, and have enhanced resources in health care fraud hot spots. The number of pending FBI investigations has shown steady increase from nearly 600 pending cases in 1992 to over 2,400 cases FY2008. FBI led investigations resulted in nearly 700 criminal health care fraud convictions and over 800 indictments and information being filed in FY 2008. The Department of Justice estimates that since the inception of the Health Care Fraud and Abuse Control program (HCFAC) in 1997, the Department of Justice has obtained more than \$14.3 billion in total recoveries, which include criminal fines and Federal and State civil settlements in health care matters, predominantly involving losses to the Medicare program. The HCFAC program funding was used to support 769 FBI positions (460 Agent, 309 Professional Support) in FY 2008.

The FBI also continues to vigorously investigate Intellectual Property crime. In early 2009, the FBI received funding which enhanced the FBI's Intellectual Property Rights (IPR) program. This will allow 31 new FBI Agents to be hired to specifically investigate and oversee IPR violations. This funding also supports the standing up of an IPR Unit to be co-located at the Department of Homeland Security (DHS) led Immigration and Customs Enforcement (ICE) IPR National Coordination Center in Crystal City, VA. The IPR Unit will include five Special Agents tasked with conducting interagency IPR investigations with prosecutive support from Department of Justice Computer Crimes and Intellectual Property Section attorneys. Participation in the IPR will assist in the de-confliction of IPR investigations with other the participating agencies.

The IPR Unit will be tasked with spearheading two high priority major case initiatives, Fractured Skies and Engine Newity. Fractured Skies will focus on counterfeit or substandard aircraft components while Engine Newity will focus on counterfeit automotive parts. Both initiatives are multi-divisional, multi-agency efforts to address dangerous health and safety related IPR violations.

The co-location of the IPR Unit will strengthen the FBI's coordination efforts with several government agencies who share a concern regarding the proliferation of counterfeit goods. These agencies include the US Patent and Trademark Office, US Department of Commerce, US Chamber of Commerce, and domestic and foreign law enforcement agencies.

### **C. Other Crimes**

While Americans justifiably worry about terrorism and white collar crimes, other crimes also impact their daily lives. We understand that national security is as much about stopping crime on our streets as it is about preventing terrorism.

Taking this on requires us to squaring priorities within existing resources. We currently have roughly a 50/50 split in resources between national security and criminal programs. To make the best use of these resources, we will continue to focus on those areas where we bring something unique to the table, and to target those criminal threats against which we will have the most substantial and lasting impact. In addition to public corruption and economic crimes, we investigate many other forms of criminal behavior including violent crime, gangs, criminal enterprises and crimes against children.

Data from the Uniform Crime Report indicates that violent crime continued to decline across the country in 2008. But this may not reflect what is actually happening on the streets, particularly in small to mid-size cities. Street-level crime is a key concern, with gang violence and gun crime largely to blame.

Since 2001, our gang cases have more than doubled. This increase did not happen by chance. Our National Gang Intelligence Center (NGIC) has been a significant source of actionable gang information. We have agents assigned full time to the Department's analytical and operational arm, the National Gang Targeting, Enforcement & Coordination Center (GangTECC), and we work closely with the Department's dedicated gang prosecutors at Gang Unit. We have more Safe Streets Task Forces in more mid-size cities. We have more than 200 Safe Streets, Gang, Violent Crime, Safe Trails, and Major Theft Task Forces across the country, with more than 850 FBI agents. And we continue to work in tandem with our state and local partners to provide a balance between immediate responses to surges in violent crime and long-term solutions.

We are deeply concerned about the high levels of violence in Northern Mexico. All too often, this violence can be traced back to three things: drugs, human smuggling, and cartel and gang activity. Because gangs are a transnational threat, the FBI formed the MS-13 National Gang Task Force. These agents and analysts coordinate investigations with our counterparts in Mexico and Central America.

Of course, drug-related violence is not new to the border area. But there have been shifts in alliances among Mexican drug trafficking organizations. These Mexican cartels are vying for control over lucrative smuggling corridors across the Southwest

border, leading to increasingly violent competition between and within Mexican drug trafficking organizations.

Mexican authorities continue their efforts to cut off drug smuggling routes from Mexico to the United States. Under President Calderon, and with support from the United States, the government of Mexico has made record seizures of drugs, clandestine laboratories, and cash. Mexican law enforcement agencies have arrested many high level drug cartel members who are being extradited to face prosecution in the United States in record numbers. One of the consequences of their efforts has been a surge in violent crime, particularly drug-related homicides in Mexico. As law enforcement cracks down on these drug trafficking organizations, the traffickers often turn against each other and against government authorities. The cartels are engaging ever more heatedly in the types of violent crime frequently associated with drug trafficking, such as murder, extortion, and kidnappings.

To address the surge in kidnappings, the FBI works closely with Mexican police officials on a Bilateral Kidnapping Task Force, as well as other ad hoc task forces and working groups along the border. To combat drug-related violence, FBI agents work with DEA, ATF, and DHS and participate on Organized Crime and Drug Enforcement Task Forces and strike forces, which target the most significant drug trafficking organizations in the region.

We have created Southwest Intelligence Group and located it in the same building as the DEA's El Paso Intelligence Center. Our intelligence group will serve as a clearing house for all intelligence related to Mexico, and provide analysis relating to crime along the border.

In sum, we are taking what we have learned about intelligence and we are applying it to criminal investigations. Rather than focusing on the number of arrests, indictments, and convictions, we are focusing on the intelligence we need to prevent crime in the first place. And we are maximizing our resources by working with partners here at home and abroad.

#### **IV. Global Reach of the FBI**

Like other federal agencies, we are worried about the economic downturn and the impact on criminal and terrorist threats against the United States. But at the same time, we understand that our role cannot be limited to the domestic front. The FBI's global role is primarily to address these threats. While there are no borders for crime and terrorism and there can be no borders for justice and the rule of law, borders are far from irrelevant.

Through our 61 Legal Attaché offices around the world, our international training programs, and our joint investigations, we have strengthened our relationships with our international law enforcement partners and expanded our global reach.

Global cooperation is not merely the best way to combat global crime and terrorism, it is the only way. And we must cooperate not only with our international law enforcement and intelligence partners, but with our private partners as well.

Consider cyber crime, for example. As the world grows more dependent on information technology systems, keeping these systems viable and secure has become an increasingly urgent national priority. Our increased reliance on technology has created

an irresistible target for criminal activity, and that activity is by no means limited to the United States.

Currently, the largest source of transnational cyber crime is Eastern Europe. Annual estimated loss to financial institutions in responding to these attacks exceeds \$200 million in the United States alone.

To combat this growing threat, the FBI has developed close working relationships with law enforcement partners within high-value target countries such as Russia and Romania, and also with allies who are victimized by these cyber criminals. We have close working relationships with countries such as Australia, New Zealand, Canada, the United Kingdom, Italy, the Netherlands, Germany, France, Poland, Estonia, and Japan, and these partnerships are paying off.

For example, in November of last year, cyber criminals executed a highly sophisticated scheme to defraud a major payment processor. Hackers gained access to the network of this payment processor and increased the funds available for a small number of payroll debit cards.

In less than 24 hours, more than \$9 million was withdrawn in connection with more than 14,000 automated teller machine transactions in 28 different countries, from the Ukraine to the United States, Canada, Italy, and Japan, among others. To date, there are more than 400 known victims, and the investigation is ongoing.

From a law enforcement perspective, the ability to respond to these attacks is hampered by their scale and their international scope. We simply cannot address this problem alone in its entirety. The growing global threat will continue to pose problems so long as attacks continue from technically sophisticated, underemployed, underpaid



actors operating from countries whose diplomatic relations with the United States may be less than ideal.

We also confront a patchwork of laws, regulations, and private industry requirements – all of which prohibit reporting and investigation on an international scale. By extension, a lack of reporting of such security breaches inhibits information sharing and hampers law enforcement and private industry in the long run.

Global cooperation addressing these cyber threats would better equip victim organizations and support a comprehensive and unified approach by law enforcement, giving us the means to leverage the collective resources of many countries. A global response will ensure deterrence, enhance confidence, and increase security in the long run. For these very reasons, we will continue to build partnerships with our international law enforcement and intelligence counterparts, and our private sector partners as well. And we will continue to investigate these kinds of transnational threats to the fullest extent of our reach and our capability.

## **V. Conclusion**

Over the past 100 years, the FBI has earned a reputation for protecting America that remains unmatched. Many of our accomplishments over the past seven years are in part due to your efforts and your support, and much of our success in the years to come will be due to your continuing support. From addressing the growing gang problem to creating additional Legal Attaché offices around the world, to compensating our personnel and protecting the American people from terrorist attack, you have supported our mission and our budget requests.

Mr. Chairman, I would like to conclude by thanking you and this Committee for your service and your support. On behalf of the men and women of the FBI, I look forward to working with you in the years to come. I would be happy to answer any questions you may have.