Testimony of

The Honorable Robert S. Mueller, III

Director
Federal Bureau of Investigation
December 6, 2006

Testimony of Robert S. Mueller, III
Director, Federal Bureau of Investigation
Before the Senate Judiciary Committee
December 6, 2006

Good morning, Mr. Chairman, Senator Leahy, and members of the committee. I am pleased to be here today to discuss the progress of the FBI's transformation efforts.

When I was sworn-in as the sixth Director of the FBI on September 4, 2001, I was aware of the need to address a number of management and administrative challenges facing the Bureau at that time. However, the terrorist attacks of September 11, 2001, the emerging threats brought on by globalization and advances in technology, and the continued traditional criminal threats, required far more changes than we could have ever expected. Indeed, the last five years have been a time of unprecedented change for the FBI.

While there have been some setbacks along the way, there has also been remarkable progress. Today, the FBI is a stronger organization, combining greater capabilities with the longstanding commitment to the security of the United States.

After the September 11th attacks on America, the FBI priorities shifted dramatically. Our top priority became the prevention of another terrorist attack. Today, our top three priorities - counterterrorism, counterintelligence, and cyber security - are all national-security related. To that end, we have made a number of changes in the Bureau, both in structure and in the way we do business. This summer we announced the realignment of our organizational structure to create five branches: National Security, Criminal Investigations, Science and Technology, the Office of the Chief Information Officer and Human Resources. These changes address areas where we and outside advisors identified weaknesses or areas where additional change is needed. This structure will carry the FBI into 2011 and beyond.

Understandably, much of the focus on the FBI in the last five years has been on the transformation, the changes, the shifts. But amid all the change, there is another story - that of tremendous accomplishment.

My testimony today is a collection of some of the FBI's most important accomplishments over the last five years. Credit for these accomplishments goes to many. The support and guidance provided by the Congress has been invaluable. The Administration has strongly supported our

efforts, and many independent organizations offered important advice and guidance that substantially enhanced our efforts.

But most of the credit, Mr. Chairman, goes to the 30,000 men and women of the FBI. They are the ones who have built on the foundation laid by the many Agents and professional staff who came before them. They are the ones who have made all that we have done in the last five years possible. And they are the ones who will be there in the future continuing the proud tradition of the FBI to protect the nation while preserving civil liberties. I have been privileged to work with this outstanding group of public servants for the last five years. Their hard work, dedication, and resolve are a daily inspiration.

As set forth below, each branch of the FBI -- National Security, Criminal Investigations, Science and Technology, the Office of the Chief Information Officer, and Human Resources -- has demonstrated the ability and the willingness to embrace change for a better, stronger, more effective FBI. These accomplishments are by no means exhaustive, but they provide a vivid illustration of the extraordinary work done day-in and day-out at the FBI.

National Security

Since September 11, 2001, the FBI has implemented significant changes to integrate our intelligence and operational elements and enhance our ability to counter today's most critical threats. We have built upon our established capacity to collect information and enhanced our ability to analyze and disseminate intelligence. Development of the National Security Branch (NSB) has been another step in enhancing the FBI's mission as a dual law enforcement and intelligence agency.

The National Security Branch structure took effect on September 12, 2005, in response to a directive from the President to the Attorney General. The NSB consists of the FBI's Counterterrorism Division (CTD), the Counterintelligence Division (CD), the Directorate of Intelligence (DI), and the new Weapons of Mass Destruction (WMD) Directorate. Combining our national security workforce and mission under one leadership umbrella enhances our contribution to the national intelligence effort and provides us with the opportunity to leverage resources from our U.S. Intelligence Community (USIC) partners, as well as our federal, state, local, and tribal law enforcement partners.

Counterterrorism Division

The mission of the Counterterrorism Division is to identify and disrupt potential terrorist plots by individuals or terror cells, freezing terrorist finances, sharing information with law enforcement and intelligence partners worldwide, and providing strategic and operational threat analysis to the wider intelligence community. Since the September 11th attacks, we have dramatically strengthened our ability to combat terrorism and have had success identifying, disrupting and dismantling terrorist threats. Set forth below are a few examples of the myriad successes in this regard.

In the past five years, we have disrupted terrorist financing mechanisms.

An investigation titled "Operation Blackbear" was initiated in 2001 and focused on three individuals involved in raising money for terrorist organizations. Our investigation identified other individuals in the United States that could remit money to Yemen for support of terrorist organizations. We developed evidence that indicated the subjects were engaged in providing money to support mujahadeen fighters in Afghanistan, Chechnya and Kashmir and that they had met with Bin Laden and provided money, arms, and recruits. Two of the subjects were arrested in Germany in January 2003 and charged with providing material support to terrorism and conspiracy to provide material support. They were extradited to the United States and indicted in December 2003. These individuals were found guilty in March 2005 and sentenced to significant prison terms. In addition, other individuals were arrested on charges such as illegal money remitting and bank structuring charges and were convicted or pled guilty in connection to this investigation. "Operation Blackbear" also resulted in the criminal forfeiture of approximately 25 million dollars.

In December 2001, an investigation into the Global Relief Foundation (GRF) proved that the organization was providing material support to terrorism. The GRF was an Islamic charity claiming to be a conduit for directing aid to the poor and needy of the Islamic world. The investigation uncovered facts to indicate that GRF was actually a conduit for funding Islamic Fighters engaged in battle throughout the world, including Chechnya. GRF was the second largest Islamic Non Governmental Organization (NGO) operating in the U.S. and was named a "Specially Designated Global Terrorist" entity by the Department of Treasury pursuant to Executive Order 13224. Through our efforts and those of our partners, this organization was successfully disrupted and dismantled. Rabih Haddad, GRF's Chairman of the Board, was subsequently arrested by INS and deported to Lebanon after a two year detention period.

In August 2003, Enaam Arnaout, Chief Executive Officer (CEO) of the Benevolence International Foundation (BIF), was convicted of racketeering conspiracy in the diversion of charitable donations to Islamic Fighters, and sentenced to over 11 years in federal prison. BIF was also an Islamic charity claiming to be a conduit for directing aid to the poor and needy of the Islamic world. The investigation uncovered facts to indicate that it was actually a conduit for funding Islamic Fighters engaged in battle in Chechnya, Bosnia, and Sudan. BIF also employed several high-ranking Al Qaeda operatives and facilitated the international travel of these individuals under the guise of charity work. BIF was third largest Islamic NGO operating in the U.S. and, like GRF, was named a "Specially Designated Global Terrorist" entity by the Department of the Treasury pursuant to Executive Order13224. This designation was based primarily upon information gathered through the FBI investigation. Due to the Treasury designations of BIF and GRF, both organizations have closed all operations in the U.S. and abroad.

Working with our federal, state and tribal partners, we have had other operational successes that contribute to the overall goal of keeping America safe.

In 2002, we arrested Iyman Faris, an Ohio truck driver from Kashmir, who later pled guilty to providing material support and resources to Al Qaeda. Faris admitted that he met with bin Laden at a training camp in Afghanistan and that he cased the Brooklyn Bridge with an eye toward planning an attack. He was sentenced to twenty years in prison.

The investigation known as the "Lackawanna Six" determined that shortly before the 9/11 terrorist attacks, specific individuals attended or supported attendees at the Al-Farooq terrorist training camp, an Al Qaeda military-style training camp, located in Afghanistan. The investigation successfully identified and documented the methods Al Qaeda members used to communicate with and recruit U.S. citizens of Yemeni descent to travel to Afghanistan for the purpose of military training for jihad. The investigation resulted in the convictions of the six men, all U.S. citizens of Yemeni descent. All were convicted of providing material support to Al Qaeda and conducting transactions unlawfully with Al Qaeda. They are currently serving sentences ranging from 7 to 10 years after pleading guilty in 2003. A seventh individual, who fled the United States prior to the capture and conviction of his cell, is believed to still be outside the country and is currently listed on the FBI's Most Wanted Terrorist section of the FBI website.

In August of last year, four men were indicted and charged with plotting to attack U.S. military facilities, Israeli government facilities, and Jewish synagogues in the Los Angeles area. Investigators broke this case when the terrorists committed a series of gas station robberies in the Los Angeles area to raise the money to finance the attacks. Together, hundreds of investigators from the FBI, state and local law enforcement, the Department of Homeland Security and other agencies worked around the clock at an FBI command post to identify other members of the cell. They spent thousand of hours tracing the steps of these terrorists until the entire cell was exposed.

Likewise, earlier this year, we worked with our partners on the Joint Terrorism Task Force in Toledo, Ohio, and with the United States Secret Service to arrest three men on charges of conspiring to commit terrorist acts against Americans overseas. These men have been charged with providing financing, computers and communications equipment to terrorists.

More recently, we worked with British and Pakistani law enforcement and intelligence authorities to investigate potential ties in the United States to the British suspects arrested in August in connection with the plot to bomb several jet airlines over the Atlantic Ocean. Together, we were able to identify the key members of this cell and stop them before they could strike.

The FBI is the lead agency for preventing and investigating domestic terrorism, such as animal rights extremism, environmental extremism, right wing and left wing extremism.

The mission of the FBI's domestic terrorism program is to identify, prevent, and defeat terrorist operations before they occur, and in the event of an act of terrorism, to fulfill its role as the Lead Federal Agency for crisis response, functioning as the on-scene manager for the United States Government. The FBI investigates and counters the activities of persons or organizations who, without foreign direction, conspire of engage in criminal activity to effect political or social change in the United States. Some examples of the FBI's domestic terrorism successes follow.

Between 1996 and 1998, bombs exploded four times in Atlanta, Georgia and Birmingham, Alabama, killing two, injuring hundreds and setting off what turned out to be a five-year manhunt for the suspected bomber Eric Rudolph. Working with federal, state and local partners through the Southeast Bomb Task Force, investigators remained focused on western North Carolina where Rudolph was believed to be living. Rudolph was captured in May 2003 in

Murphy, North Carolina by a local officer who spotted him rummaging through a dumpster. Rudolph signed a plea agreement in April 2005, pleading guilty to both the Birmingham bombing and the Atlanta bombings. In connection with the plea agreement, five caches, containing approximately 265 pounds of dynamite and other bomb making material, were recovered in western North Carolina. In July 2005, Rudolph was sentenced to two consecutive life terms for the two counts in the Birmingham bombing.

A series of Earth Liberation Front (ELF) arsons occurred in the Sacramento, California, area beginning in December 2004, when four improvised incendiary devices (IIDs) were discovered at a construction site in Lincoln, California. In January 2005, five IIDs were discovered at a construction site in Auburn, California. In February 2005, seven IIDs ignited in an apartment complex under construction in Sutter Creek, California. Based on source information and follow-up investigation, four individuals were arrested. Charges included conspiracy to commit arson and aiding and abetting arson. All of the subjects ultimately pled guilty and are serving sentences ranging from two to six years incarceration.

In January 2006, a 65 count indictment of 11 individuals was handed down on charges including arson and destruction of an energy facility on behalf of the Earth Liberation Front and Animal Liberation Front movements (ALF/ELF).

These and other investigations demonstrate the advancements that the FBI counterterrorism program have made in the last five years. Our counterterrorism efforts are enhanced in other ways as well.

Joint Terrorism Task Forces

Joint Terrorism Task Forces (JTTFs) team up police officers, FBI agents, and officials from over 20 federal law enforcement agencies to investigate terrorism cases. We have increased multi agency Joint Terrorism Task Forces (JTTFs) from 35 to 101 since 2001, and have increased the number of Agents and law enforcement serving on JTTFs from under one thousand to nearly four thousand. To support the JTTFs, thousands of clearances have been processed for state/local JTTF officers. The JTTFs have been a resounding success, and they play a central role in virtually every terrorism investigation, prevention, or interdiction within the U.S.

These local force multipliers are mirrored at Headquarters with the National Joint Terrorism Task Force (NJTTF). Immediately following the attacks of September 11, 2001, an ad hoc group of representatives from federal agencies began meeting, sharing information, and working together in the FBI's Strategic Information Operations Center at Headquarters. In July 2002, we formally created the NJTTF to act as a liaison and conduit for information on threats and leads from FBI Headquarters to the local JTTFs and to 40 participating agencies. The NJTTF now includes representatives from members of the Intelligence Community; components of the Departments of Homeland Security, Defense, Justice, Treasury, Transportation, Commerce, Energy, State, and the Interior; the City of New York Police Department; the Nuclear Regulatory Commission; Railroad Police; U.S. Capitol Police; and others. All members are provided with access to the FBI intranet, including its internal e-mail system, and to the FBI's investigative database for

purposes of counterterrorism investigations. In turn, members provide access to their organizations' respective databases consistent with applicable laws and regulations.

Terrorist Screening Center

On September 16, 2003, the President directed the Attorney General, Secretary of Homeland Security, Secretary of State, and Director of Central Intelligence to develop the Terrorist Screening Center (TSC) to consolidate information from terrorist watch lists and provide 24-hour, seven-days-a-week operational support for law enforcement, consular officers and other officials. The FBI was directed to lead this effort and we began operations in December 2003.

The TSC manages the one, consolidated terrorist watchlist, providing key resources for screeners and law enforcement personnel. These include: a single coordination point for terrorist screening data; a 24/7 call center for encounter identification assistance; access to a coordinated law enforcement response; a formal process for tracking encounters; feedback to the appropriate entities; and a process to address misidentification issues. Recent TSC successes include: a traffic stop resulting in the arrest of a suspect connected to Hamas, which is denoted as a Specially Designated Terrorist Organization by the Department of State, and a customs in-flight check with the FBI prompting an arrest at the Chicago Airport.

Foreign Terrorist Tracking Task Force

The Foreign Terrorist Tracking Task Force (FTTTF) was created pursuant to Homeland Security Presidential Directive No. 2 and was consolidated into the FBI pursuant to the Attorney General's directive in August 2002. The FTTTF uses innovative analytical techniques and technologies that help keep foreign terrorists and their supporters out of the United States or lead to their location, detention, prosecution, or removal. The participants in the FTTTF include the Department of Defense, the Department of Homeland Security's Bureaus of Immigration and Customs Enforcement and Customs and Border Protection, the State Department, the Social Security Administration, the Office of Personnel Management, the Department of Energy, and the Central Intelligence Agency. FTTTF has also established liaison with foreign partners including Canada, Australia, and the United Kingdom. To accomplish its mission, the FTTTF has facilitated and coordinated information sharing agreements among these participating agencies and other public and proprietary companies to assist in locating terrorists and their supporters who are, or have been, in the United States. The FTTTF has access to over 40 sources of data containing lists of known and suspected foreign terrorists and their supporters, including the FBI's Violent Gang and Terrorist Offenders File (VGTOF).

Counterintelligence Division

Foreign counterintelligence (FCI) is a crucial component of the FBI's overall strategy, second only to counterterrorism. As the lead agency for FCI in the United States, and the primary investigative component of the Department of Justice, the FBI has the responsibility to oversee the integration of U.S. law enforcement and intelligence efforts to ensure that all available means

are brought to bear to mitigate this ongoing and daunting threat, consistent with our laws and policy.

In February 2002, the FBI embarked on a dramatic transformation of its Counterintelligence program. Awareness of the growing threat to United States national security interests, combined with a realization that adversaries were successfully expanding their efforts, utilizing new approaches, and targeting critical United States technologies forced a comprehensive reconsideration and redirection of the FBI's Counterintelligence program. The FBI's Counterintelligence program has been transformed and, while continuing to show success against traditional adversaries, has developed and implemented a far-reaching program designed to address a new and growing threat that seeks to disadvantage the United States in virtually all sectors and every section of the country.

While many of our counterintelligence successes cannot be discussed publicly, the following cases represent some of our efforts to address this threat.

The FBI recently concluded a major counterintelligence investigation involving Lawrence Franklin, a former Iran desk officer in the Office of the Secretary of Defense at the Pentagon. Franklin, from Kearneysville, West Virginia, was sentenced on January 20, 2006, by U.S. District Judge T.S. Ellis III on three felony counts: conspiracy to communicate national defense information to persons not entitled to receive it; conspiracy to communicate classified information to an agent of a foreign government; and the unlawful retention of national defense information. Franklin was sentenced to a total of 151 months in prison and ordered to pay a fine of $10,000.

On December 15, 2005, a federal jury convicted Kenneth Wayne Ford, Jr., of Waldorf, Maryland, of unlawfully possessing classified information related to the national defense and making a false statement to a U.S. government agency. Ford was employed by the National Security Agency (NSA) between June 2001 and late 2003. On January 11, 2004, FBI agents executed a search warrant at Ford's residence and discovered sensitive classified information throughout his home, including numerous Top Secret documents in two boxes in Ford's kitchen. Ford was arrested on January 12, 2004. Ford had taken home the classified information on the last day of his employment at NSA in December 2003, when Ford was to start working in the private sector on a classified contract for a defense contractor. On March 30, 2006, Ford was sentenced to 72 months in prison.

On March 23, 2006, Howard Hsy, of Bellevue, Washington, was sentenced by a U.S. District Court Judge to two years of probation and a $15,000 fine for conspiracy to violate the Arms Export Control Act. Hsy conspired with others to export night vision goggles and camera lenses to a contact in Taiwan. Exporting those items required a license and written approval from the State Department, which Hsy did not have. The military equipment is later shipped to the People's Republic of China. Hsy conspired with others in the Seattle area and Taiwan to purchase the military gear for export. The military equipment was primarily used by military pilots to fly and navigate at night. In October 2005, a Seattle-area co-conspirator, Donald Shull, pled guilty to

conspiracy to violate the Export Administration Act and was sentenced in February 2006 to two years of probation and a $10,000 fine.

On January 25, 2006, the U.S. Southern District Court of Indiana convicted Shaaban Hafiz Ahmad Ali Shaaban of six counts: conspiracy; acting as a foreign agent without notification; one violation of the Iraqi Sanctions under the International Emergency Economic Powers Act; unlawful procurement of an identification document; and unlawful procurement of naturalization. Shaaban never registered as an agent of Iraq, yet, in 2002 and 2003 when he lived in Indianapolis and Greenfield, Indiana, Shaaban traveled to Baghdad in late 2002 where he offered to sell names of U.S. intelligence agents and operatives to Iraq for $3 million; sought to gain Iraqi support to establish an Arabic television station in the United States that would broadcast news and discussions that would be pro-Iraqi; sought to enter into a "cooperation agreement" where he would be paid a fee by Iraq to organize volunteers to act as human shields to protect Iraqi infrastructure during the war; and broadcasted messages of support for the Iraqi government on Iraqi media stations that advocated support for Iraq and encouraged others to forcibly resist the United States and others who opposed Iraq.

Counterintelligence Operations

The Counterintelligence Division (CD) has implemented the National Strategy for Counterintelligence (National Strategy), focusing resources on counterproliferation, counterespionage, and protection of critical national assets. This included implementation of field office counterintelligence program reviews utilizing metrics tied to the National Strategy, ensuring resources in the field are prioritized and following the National Strategy, recommending improvements where needed.

CD has also established a Counterespionage Section to focus and consolidate espionage investigations within one section at headquarters. They seek to identify and investigate the non traditional foreign intelligence threat in both establishment and non establishment offices. It also has developed country specific program directives to the field offices that are coordinated by headquarters.

Training and Workforce

The CD agent workforce now constitutes a sizable portion of the overall agent workforce, receiving steady enhancements since 2002. With this larger workforce, we have established CD squads in all 56 field offices. Additionally, we use contractors with counterintelligence expertise to augment the program where needed.

The Counterintelligence Training Center (CITC) has also expanded, which has doubled the number of trained counterintelligence professionals. We have also expanded advanced training programs, and have seen a significant increase of the number of agents who received this advanced training. Also of note is the establishment of a CD supervisors course and a CD field executive course.

Outreach and Coordination

We have helped establish the National Counterintelligence Working Group, an inter agency group of 25 national level CI leaders, which, with the FBI, coordinates counterintelligence operations at the national level. We have also established regional inter agency counter-intelligence working groups throughout the U.S., which, with the FBI, implement the National Strategy by reviewing joint operations, identifying priorities and trends, and providing a general forum for agency de confliction.

We have focused on working with those who may be targets of foreign counterintelligence efforts. We established joint technology protection task forces with DOD to protect specific weapons systems such as the Joint Strike Fighter. We implemented an "Agents in the Lab" program in specific DOE facilities for the purpose of raising counterintelligence awareness and broadening the FBI's access to intelligence within the labs.

Our newly-established Domain Section within the FBI focuses resources on building relationships in business and academia through Business and Academic Alliances. We have secured the cooperation of major corporations such as L3, Boeing, Northrup Grumman, Lockheed Martin, and Tier 1 research universities in our domain initiative.

We will also soon release our Research Technology Protection/Infragard website that will support information sharing by providing unclassified FBI, DOD, and Defense Security Service intelligence products to cleared contractors, academia, and interested businesses.

Directorate of Intelligence

In 2005, the FBI created its Directorate of Intelligence, which is responsible for intelligence policy within the Bureau and controls the budget for the people, information technology, training, and other resources that it manages. The Directorate succeeded the Office of Intelligence, which we stood up following the September 11, 2001, terrorist attacks. In response to today's asymmetic threats, we have elevated our intelligence program to a level on par with our investigative programs. The new intelligence program is defined by enhanced analytical capabilities, state of the art information technology and an integrated intelligence structure at headquarters and in the field.

Intelligence Career Service

The FBI has created an Intelligence Career Service (ICS) of FBI Special Agents, Intelligence Analysts, Language Analysts, and Physical Surveillance Specialists whose members work in every FBIHQ division and all 56 field offices. We have embedded analysts, or are taking actions to do so, in the FBI Laboratory, Operational Technology Division, Criminal Justice Information Services, and Special Technologies and Applications Office to explore and exploit unique information available that is responsive to national requirements. The DI continues to build up the ICS, bringing onboard 370 additional Intelligence Analysts (IAs) in fiscal year (FY) 2006; the FBI currently has over 2,100 IAs on board through these efforts.

To support the ICS, we have established training in order to achieve a consistent level of knowledge across the workforce on intelligence concepts and processes. Training remains a

major focus of the DI's efforts in 2006, with improvements in the Analytical Cadre Education Strategy (ACES) and implementation of an aggressive schedule to provide training to IAs, Language Analysts (LAs), and surveillance personnel in cohort groups as they are hired. Cohort training, which replaces ACES 1.0 for new ICS hires, began on October 16, 2005, with two pilot classes. ACES training is mandatory for all onboard IAs.

To date, we have trained 392 ICS personnel through Cohort, and have trained over 2,000 ICS personnel through ACES. However, we also recognize a clear need to aggressively work to improve training, if we are to meet workforce expectations and mission demands. Therefore, we are implementing a specific action plan with the FBI's Training and Development Division, in cooperation with our Community partners, to advance FBI training into an environment consistent with the demonstrated readiness of our workforce and our mission demands.

In December 2005, we certified the first FBI Intelligence Officers as part of the pilot implementation of the FBI Intelligence Officer Certification (FIOC) Program. FBI Intelligence Officer Certification is a credential that recognizes achievement in and long term commitment to the intelligence profession as demonstrated through experience, education, and training. Eleven FBI executives have been certified, on the basis of prior training and activities.

Linguists/Languages

The FBI has increased its overall number of linguists by 82%, with the number of linguists in certain high priority languages (Middle Eastern and North African languages) increasing by more than 250%. Our hiring efforts are ongoing, with over 100 Language Analysts in the final hiring process and a significant number of prospective full time candidates identified from current Contract Linguist applicants. The 2006 Budget provided an additional 264 full time linguist positions for a total of 694 Language Analyst positions. In addition to Language Analyst positions, many field offices will be receiving new or additional supervisory positions to accommodate and manage the growing FBI linguist population.

To ensure that all FBI linguists are subject to at least an annual quality control review, we have established a translation Quality Control program in our Language Services Section (LSS). In addition, all translations presented in court or otherwise designated for public release, as well as the first 40 hours of translation work performed by new linguists after their initial training period, are subject to full quality control review.

LSS has trained and certified more than 201 quality control reviewers from the middle of 2005 to the end of June 2006, and continues to conduct Quality Control Reviewer Workshops on an almost monthly basis to increase and retrain linguists certified to conduct quality control reviews. There have been 2755 Quality Control reviews performed since the inception of the program.

Finally, the FBI is the designated Executive Agency for the National Virtual Translation Center (NVTC), established under the authority of the USA PATRIOT Act to "provide accurate and timely translations of foreign intelligence material to the US intelligence community." The NVTC is the element of the United States government specifically dedicated to the timely and accurate translation of foreign intelligence for US government agencies. In addition, it enables

interagency sharing of translation resources, maximizes human and automated translation capabilities, and balances the workload of translation jobs among the various IC elements.

Field Intelligence Groups

We have developed and directed the implementation of the Field Intelligence Group (FIG) program, which serves as the lens through which the Field Divisions evaluate threats. The FIG is the mechanism through which the FBI contributes to regional and local perspectives on a variety of issues, to include the receipt of and action on integrated investigative and intelligence requirements. FIGs further provide the intelligence link to the Joint Terrorism Task Forces, Fusion Centers, FBIHQ and the Intelligence Community at large. FIGs, which have been established in all 56 Field Offices since October 2003, consist of Intelligence Analysts, Special Agents, Language Analysts, and Special Surveillance Groups. FIG personnel have been embedded in more than twenty-five Fusion Centers and/or Multi Agency Intelligence Centers (MAICs) around the country.

Sharing Intelligence

Among the fundamental post September 11th changes, sharing intelligence is now the main objective. We have developed an FBI intelligence presence within the intelligence and law enforcement communities by sharing Intelligence Information Reports (IIRs), Intelligence Assessments (IAs), Intelligence Bulletins (IBs), and related intelligence information on platforms routinely used by our law enforcement and Intelligence Community partners, including JWICS, SIPRNet and LEO, as well as on the FBI Intranet. This effort has resulted in more than 7,400 IIRs, 150 IBs, and 100 IAs that have been posted on all listed platforms; in addition, over 400 Current Intelligence Reports have also been produced, of which over 50 have been shared with the intelligence community through NCTC Online. Furthermore, we are using our internal, closed network to provide FBI employees with access to raw, current and finished intelligence.

Domain Management Initiative

We recently began implementing the National Security Branch (NSB)'s Domain Management Initiative, a methodological approach to FBI mission management that will define our National Security mission and, by extension, our Criminal and Cyber missions. Traditionally, the FBI has derived intelligence primarily from our cases. The stand up of the NSB in 2005 required that we expand our intelligence capacity beyond case driven investigations. The focus is to remain ahead of the threat.

The goal of Domain Management is to develop a comprehensive understanding of a territory's threats and vulnerabilities so that managers can effectively deploy resources for greatest impact. Domain Management is simply about "questions and choices": What do you need to know about your territory to protect the people in it? What do you know about the threats and vulnerabilities that worry you most? What don't you know about the threats and vulnerabilities that worry you most? What are you going to do to address your threats and vulnerabilities?

Weapons of Mass Destruction

The FBI serves as the lead agency for the investigative, intelligence, counterintelligence, and overall law enforcement response to a terrorist threat or incident in the United States, and is charged with lead agency responsibility for investigating violations of weapons of mass destruction (WMD)-related statutes. A critical, challenging part of this mission is to detect and disrupt the acquisition and use of WMD.
We recently created a WMD Directorate (WMDD) within our National Security Branch. The strategic focus of this Directorate is to prevent and disrupt the acquisition of WMD capabilities and technologies for use against the United States. The WMDD will support and consolidate the FBI's WMD components. The strategic focus of this Directorate is to prevent and disrupt the acquisition of WMD capabilities and technologies for use against the U.S. homeland by terrorists and other adversaries, including nation-states. It integrates and links all of the necessary counterterrorism, intelligence, counterintelligence, and scientific & technological components to accomplish the FBI's overall WMD mission.

Over the past five years, the FBI's WMD components have engaged in outreach to target specific sectors of industry, such as the chemical and agricultural industries, to increase WMD awareness and sensitivities to potential threats and to facilitate reporting of information that potentially has intelligence value. This includes the establishment of a two-way communication and methods to report suspicious activity. WMD components established two WMD-specific InfraGard portals to provide unclassified information and intelligence products to vetted academia and industry members.

Criminal Investigations

National security is the top priority of the FBI, and must remain so. To support our top priorities of counterterrorism and counterintelligence, we have shifted Special Agents to those programs from criminal investigative programs. Nevertheless, our criminal investigative program remains effective.

In the last five years, we have focused our resources on those areas where the FBI has unique and specialized capabilities. From cyber crime to public corruption to white collar crime and beyond, the number of successful and important investigations are significant. Our criminal investigative program may be relatively smaller than it was five years ago, but its impact is greater than ever.

Cyber

Shortly after the September 11, 2001, terrorist attacks, the FBI established as our third priority protecting the United States against cyber-based attacks and high-technology crimes. In coordination with this priority and recognition of the international aspects and national economic implications of cyber threats, the FBI created a Cyber Division (CyD) at the headquarters level to manage and direct this nationally developing program.

The rapid evolution of computer technology, coupled with ever increasing techniques used by terrorists, foreign intelligence actors, and criminals, requires FBI investigators and professionals to have highly specialized computer based skills. The FBI Cyber Program uses a centrally coordinated strategy to support FBI priorities across program lines, assisting crucial

Counterterrorism (CT), Counterintelligence (CI), and criminal investigations whenever aggressive technical investigative assistance is required. The Cyber Program also targets major criminal violators with a cyber nexus.

We have achieved significant results in both computer intrusion investigations and cyber crime investigations.

Computer Intrusions

Computer intrusion cases counterterrorism, counterintelligence, and then criminal are the first order of business due to their relationship to national security matters.

Among the most notable investigations for the Cyber Division was the successful resolution of the Zotob worm case. The Zotob worm is an IRC bot program, which manipulates infected systems to connect to a remote server for further instructions. This architecture allows the operator complete remote access to infected computers, enabling them to send SPAM, launch denial of service attacks, steal personal information, and compromise more computers. The Zotob case was initiated as a routine computer intrusion matter, but quickly transformed into a highly complex, global investigation which encompassed other CyD programs including computer fraud, child pornography, and the transmission of malicious code. In August 2005, one FBI team was deployed to Rabat, Morocco and one FBI team was deployed to Ankara, Turkey. The teams were made up of FBI investigators, FBI malicious code experts, and computer forensic experts. FBI deployment teams were provided direct access to Turkish law enforcement by Legat Ankara and Moroccan law enforcement by ALAT Rabat. Cooperation was achieved from Microsoft Corporation, major Internet service providers, and other private sector e businesses, and the CyD collaborated with law enforcement in Morocco and Turkey. As a result, the two individuals responsible for the worm were apprehended.

As the world relies even more on technology in the future, computer intrusion cases will undoubtedly grow. The FBI is committed to the continued development of its computer intrusion investigative program and building on the progress of the last five years.

Innocent Images National Initiative

The FBI also remains committed to the Innocent Images National Initiative (IINI). The IINI is an intelligence driven, proactive initiative that combats the worldwide proliferation of child pornography and child sexual exploitation facilitated by the Internet. IINI's mission is to identify, investigate, and prosecute sexual predators who use the Internet and other online services to sexually exploit children; to establish a law enforcement presence online as a deterrent; and to identify and rescue child victims.

As an example, in January of 2002 the FBI led an investigation which resulted in the rescue of a thirteen year old girl who had been taken to Northern Virginia from Pittsburgh, Pennsylvania by an individual she met on the Internet. The girl was transported across state lines and held in a residence where she was repeatedly sexually assaulted. When the girl was rescued, she was restrained to a bed post with a dog collar and a chain. The subject was

identified after bragging in an Internet chat room and sending photographs of the victim whom he identified as his "sex slave". The subject was prosecuted in the United States District Court for the Western District of Pennsylvania and sentenced to seventeen years in prison.

Since its inception in 1996, the program has grown exponentially, and in recent years the pace has increased. Between October 2002 and September 2004, more than 7,000 cases have been opened, more than 2,300 informations/indictments were issued, and nearly 2,300 convictions and/or pre-trial diversions have been secured.

In October 2004, the Innocent Images International Task Force (IIITF) was established as an initiative to target East Central European child pornography websites. The task force has generated nearly 3,000 leads that have been forwarded to the DOJ funded Internet Crimes Against Children Task Forces (ICAC) and FBI offices around the country. Almost 1,000 leads have been disseminated to our international partners in more than 67 different countries.

Internet Crime Complaint Center

A key element to many successful investigations is the assistance of the public. The Internet Crime Complaint Center (IC3) enables the public to alert us to potential cyber crimes. Since its inception, the IC3 has received over 700,000 consumer complaints, more than 450,000 of which have been referred to law enforcement for investigation. These referrals include an accumulated loss in excess of $450 million as of December 31, 2005.

As the IC3 is currently receiving over 22,000 complaints a month, the one millionth consumer complaint is expected to be processed in calendar year 2007. The IC3 has referred over 4,500 significant identified cases with an accumulative loss of $213 million to state and local law enforcement. The nearly 900 investigations that followed have resulted in 155 search warrants issued, 56 arrest warrants issued, 479 arrests, 173 indictments, and 119 convictions.

The IC3 also has coordinated several national initiatives since its inception for the advancing of investigations and prosecutions of Cyber cases, enhancing the development of productive task forces, and establishing public/private alliances to facilitate the timely sharing of intelligence. Such intelligence is vital in crafting an aggressive and proactive strategy to Cyber crimes, both domestically and internationally. Initiatives include Operation Cyber Loss, Operation E Con; Operation Cyber Sweep and Operation Web Snare. These initiatives found more than 1.1 million victims and resulted in more than 400 investigations, 263 indictments, 293 search/seizure warrants, $604 million in losses, and 355 arrests and convictions.

As with computer intrusion cases, cyber crime cases are expected to increase in the coming years. Through the establishment of the FBI's Cyber Division and the ongoing initiatives such as the Innocent Images National Initiative, the FBI will be well-prepared to combat these growing crimes.

Criminal

Public Corruption

Public corruption is a betrayal of the public's sacred trust. It erodes public confidence and undermines the strength of our democracy. Unchecked, it threatens our government and our way of life. That is why it is our top criminal investigative priority.

Over the last two years, the FBI has convicted more than 1,060 government employees involved in corrupt activities, to include 177 federal officials, 158 state officials, 360 local officials, and more than 365 police officers. In FY 2005 alone, the Public Corruption Program saw a 25% increase in public corruption cases investigated, resulting in 890 indictments, 759 convictions, and 2,118 cases still pending. There are 622 agents currently working public corruption matters, an increase of 264 since 2002.

One investigation to note is the Phoenix Division's Lively Green investigation. This involved up to 99 indictable subjects who used their positions in the military to facilitate the smuggling of several hundred kilograms of cocaine across the U.S./Mexican border.

Violent Gangs

The FBI has increased its focus on violent gangs through its continuing Safe Streets Violent Crime Initiative. Started in 1992, Safe Streets Task Forces (SSTFs) are the primary mechanism developed for this initiative. The focus of SSTFs is to achieve maximum coordination and cooperation of the participating law enforcement agencies to investigate state and federal crimes committed by these violent gangs and others.

As of June 2006, the FBI currently operates more than 160 SSTFs in 55 FBI Field Offices which are comprised of more than 1800 local, state, and federal investigators representing more than 500 law enforcement agencies throughout the United States. Of these task forces, 129 are considered violent gang SSTFs. The 129 Violent Gang Safe Streets Task Forces (VGSSTF), which operate in 54 FBI Field Offices, represent a 38% increase in VGSSTFs since FY 2000, when SSGU operated 49 VGSSTFs.

In 2004, the FBI established the MS 13 National Gang Task Force to investigate the violence associated with this gang. The MS 13 gang members are primarily from the Central American countries of El Salvador, Honduras and Guatemala and were first identified in Los Angeles in the 1980s. The threat posed by MS 13 is unique due to its strong links to the military and rebels involved in the civil wars in El Salvador, Honduras and Guatemala. The MS 13 members and associates have been identified in more than 30 states and have a significant presence in the metro areas of Houston, Los Angeles, New York City, and Washington, D.C. This task force works closely with other federal, state, and local agencies deconflicting and coordinating efforts against MS 13 gang targets. As of July 2006, there were 36 pending MS-13 Racketeering Enterprise Investigations and 58 MS-13 criminal investigations.

Innocence Lost National Initiative

The Innocence Lost National Initiative successfully addressed the crime problem of domestic trafficking of children for the purposes of prostitution. To date, this initiative has been expanded to 26 cities with an identified child prostitution crime problem. Eighteen task forces have been established with state and local law enforcement to combat this crime problem, with strong

support provided by the National Center for Missing and Exploited Children. There have been 188 investigations (child exploitation or child trafficking cases) initiated, which resulted in 574 arrests, 115 indictments and 101 convictions. Prosecution at the federal level has resulted in the dismantling of 16 criminal organizations engaged in child prostitution.

Indian Gaming

In February 2003, FBI established the Indian Gaming Working Group (IGWG). This group consists of seven federal agencies and representatives from FBI subprograms including financial crimes, public corruption, and organized crime. Since March 2004, the FBI has hosted eight IG conferences and trained more than 500 personnel assigned to work IG matters. This training and the FY 2005 enhancement contributed to the initiation of 16 IG investigations focusing on public corruption, theft, and embezzlement. As a result of the IGWG, an investigation was initiated in New York in which members of an organized crime family had infiltrated IG casinos in North Dakota and Oklahoma. Investigators learned that these members were moving large sums of money through the Indian reservations and offshore gambling operations. From 2000 2004, more than $200 million in illegal bets were placed with $65 million being wagered on horse races. In January 2006, 17 individuals were indicted and arrested.

Financial Crimes

Since October 2001, the FBI's Corporate/Securities and Commodities Fraud has remained as a priority within the White Collar Crime (WCC) Program. The outbreak of large scale corporate fraud threatened to undermine investor confidence and trust in the stock market, and financially injured millions of investors and employees. To address this significant crime problem, the FBI established a Corporate Fraud Initiative (CFI) as part of the President's Corporate Fraud Task Force. The CFI effectively focuses and coordinates the FBI's limited WCC resources on combating the corporate fraud crime problem. As a participant on the President's Corporate Fraud Task Force, and the lead agency investigating corporate fraud, the FBI has concentrated its efforts on those cases that involve accounting schemes, self dealing by corporate executives and obstruction of justice to conceal illegal activities from criminal and regulatory authorities.

Since initiating the CFI in 2001, the FBI has opened 465 corporate fraud investigations in which it is alleged that corporate officers intentionally "cooked the books" in order to artificially inflate the value of their corporation's stock and/or to justify paying themselves millions of dollars in bonuses to which they were not entitled. Major corporate fraud investigations since 2001 include Enron, Worldcom, and Qwest Communications. In addition, an emerging corporate fraud problem that the FBI is currently investigating involves allegations of the fraudulent backdating of stock options grants issued by public companies. FBI offices are working with information provided by the Securities and Exchange Commission (SEC) to investigate these matters and we currently have over 45 separate investigations on backdating.

To date, the FBI has obtained 2,962 indictments/informations, 2,569 convictions and restitution totaling over $14.9 billion related to Corporate and Securities Fraud. As of 7/27/2006, 109 FBI

agents are dedicated to Corporate Fraud investigations, with an additional 158 FBI agents working Securities Fraud investigations.

Since October 2001, the FBI's Financial Institution Fraud (FIF) Program has targeted the most egregious financial institution offenders, both insiders and outsiders.

The FBI's Mortgage Fraud Program, for example, consists of our working with approximately 200 contacts in law enforcement and industry at the national level, and task forces and contacts at the field office level, in order to address this over $1 billion crime problem. The Mortgage Fraud Program focuses our resources on those engaging in mortgage fraud for profit, as opposed to property, typically involving rings of professional insiders. In December of 2005, the FBI participated in Operation Quick Flip, a national takedown that resulted in 156 indictments, 81 arrests and 89 convictions. The losses associated with these cases alone cost the mortgage industry $607 million.

Since October 2001, the Financial Institution Fraud Program has made more than 6,000 arrests, obtained more than 13,000 indictments and informations, and secured more than 12,000 convictions. These investigations have resulted in more than $131 million in recoveries, $159 million in seizures and forfeitures, $14 billion in restitution payments, and $632 million in fines.

The Health Care Fraud Program has remained within the top five WCC Program national priorities since October 2001. The overall mission of the program is to target the most egregious health care fraud offenders, both organizations and individuals, who are defrauding the public and private health care systems. The FBI has a number of initiatives in place to combat this activity, including: the Pharmaceutical Fraud Initiative, focused on investigations that involve drug diversion, off-label marketing and prescription fraud; the Internet Pharmacy Initiative, focused on the identification of internet pharmacies involved in the illegal distribution of pharmaceuticals in the United States and internationally; the Outpatient Surgery Center Initiative which addresses the nationwide schemes in which health care providers and facilities are billing private insurance plans for unnecessary outpatient surgeries arranged through a network of individuals that includes owners of medical clinics, physicians, marketers and recruiters; and the National Automobile Accident Insurance Fraud Initiative that was developed to enhance investigations involving members of staged accident rings formed specifically to defraud health care entities. The number of pending Health Care Fraud investigations has shown steady increase since October 2001 from approximately 500 cases in 1992 to over 2,500 cases through 2005.

Partnerships with Law Enforcement

Our partnerships with foreign, state, local and tribal law enforcement have been integral to our ability to protect this nation.

Office of Law Enforcement Coordination

In May 2002, we established the Office of Law Enforcement Coordination (OLEC) to enhance coordination and communications between the FBI and its state, local, tribal, federal, and

international law enforcement partners. In just a few short years, OLEC has become central to our outreach and educations efforts for law enforcement.

OLEC developed, implemented and manages the Police Executive Fellowship Program (PEFP), a six month work exchange program for mid level and above law enforcement managers. Since its inception, 22 Fellows have served in a variety of assignments at FBIHQ, including: the National Joint Terrorism Task Force, National Gang Intelligence Center, Interpol, the Directorate of Intelligence, Law Enforcement On Line (LEO), and MS 13 National Gang Task Force.

OLEC has produced two suicide bomber broadcasts and videos which raised law enforcement partners' awareness of new trends in suicide bombings. And, in conjunction with the U.S. Department of Homeland Security and a number of state and local law enforcement agencies, OLEC produced and disseminated a roll call training video entitled, "Vigilance: Patrolling in the New Era of Terrorism." The video was sent to over 20,000 state, local and campus law enforcement agencies along with an informational brochure on terrorism indicators. OLEC continues to receive requests for both products (video and brochure).

Office of International Operations

The Office of International Operations (OIO) and the Legal Attache (Legat) Program support the FBI's core investigative priorities through liaison and operational interaction with the FBI's foreign law enforcement counterparts and overseas intelligence community. The relationships developed by the Legats are essential to the successful fulfillment of the responsibilities of the FBI. The Legat Program provides for a prompt and continuous exchange of information with foreign law enforcement and intelligence agencies enabling the FBI to effectively and expeditiously achieve its international responsibilities.

Since September 11, 2001, OIO has aggressively pursued expanding the Legat Program in an effort to identify countries/regions in critical need of new or expanded Legat offices in areas known for terrorist group development, fundraising, transit, and/or support. Additionally, in conjunction with substantive FBIHQ Divisions, OIO is attempting to identify areas, such as South America, which have historically been predominately involved in illegal drug trafficking, but are becoming increasingly involved in significant terrorist related activities. The cultural and geographic span of some of the existing Legats, such as those in Africa, is too large and should be narrowed; Legat Pretoria, for example, covers 16 countries.

In Fiscal Year 2001, there were 44 Legat offices with 112 Agent and 74 support employees for a total of 186 personnel stationed abroad. Today, the FBI has 57 fully operational Legat offices and 13 sub offices with 167 agent and 111 support personnel assigned for a total of 278 employees stationed abroad, an increase of nearly 70%.

Since September 11th, we have opened Legat Offices in Abu Dhabi, United Arab Emirates; Baghdad, Iraq; Beijing, China; Doha, Qatar; Freetown, Sierra Leone; Jakarta, Indonesia; Kabul, Afghanistan; Kuala Lumpur, Malaysia; Rabat, Morocco; Sana'a, Yemen; Sarajevo, Bosnia Herzegovina; Sofia, Bulgaria; and, T'bilisi, Georgia.

Investigative Analysts (IAs) have been placed in eight Legat offices since September 11, 2001 and the number of international students attending the National Academy (NA) at Quantico has increased by 20% in an effort to provide direct law enforcement assistance to our Legat personnel. OIO has emphasized the importance of providing financial assistance to countries and/or agencies of first time NA attendees who could not otherwise afford to attend, such as candidates from East Timor and Namibia.

Science and Technology

The FBI's science and technology capabilities have always been significant. From fingerprints to DNA analysis, the FBI has provided exceptional service to the law enforcement community. The FBI remains a leader in technical innovation and developments in the sciences that support investigative and intelligence-gathering activities.

FBI Laboratory

Investigations and intelligence gathering are the lifeblood of the FBI, and the FBI Laboratory supports those efforts. FBI Laboratory personnel routinely examine evidence from major cases, as well as other cases that do not receive publicity. Whether the case is big or small, just around the corner or halfway around the world, the FBI Laboratory approaches each one with the same steadfast determination and desire to be the world's foremost forensic laboratory upon which FBI field offices, investigative and intelligence agencies, and the American public can always rely.

Relocation to New Laboratory Facility and Re Accreditation

In 2003, the FBI Laboratory employees began moving from FBI Headquarters in Washington, DC, to its new facility in Quantico, Virginia. The Laboratory's nearly 500,000 square foot, state of the art design reveals four floors for specialized laboratories and offices and a library on the fifth floor, a 900 space parking garage, and a stand alone central utilities plant. The facility is a model for security and evidence control with specified paths for the acceptance, circulation, and return of evidence. The Laboratory successfully achieved re accreditation in its new facility from the American Society of Crime Laboratory Directors/Laboratory Accreditation Board after this significant relocation.

Terrorist Explosive Devices Analytical Center

The Terrorist Explosive Devices Analytical Center was established in 2004 to serve as the single interagency organization to receive, fully analyze and exploit all terrorist Improvised Explosive Devices (IED's) of interest to the United States worldwide, and to develop actionable intelligence to respond to the threat. The TEDAC is co located within the FBI Laboratory and as such leverages the FBI Laboratory's broad based technical and forensic capabilities along with electronic exploitation services provided through the Operational Technology Division.

The TEDAC has successfully made 56 positive identifications of bomb makers since beginning operations. In one case, a latent print developed in January 2004 on a keyless car entry system

used in an IED, was matched to a specific individual taken into custody for unrelated reasons on October 30, 2004. DNA removed from this same IED component was linked to DNA recovered in another bombing. In addition, the identified individual was linked through fingerprints to a rocket attack on the al Rashid Hotel in October 2003.

Overall, as of August 2006, the TEDAC has received over 8,670 submissions from Iraq and Afghanistan. It has developed in excess of 2,500 latent prints with over 450 matches and associations that have forensically connected one TEDAC device to another through device construction, latent prints, trace evidence (both hairs and fibers) and by DNA.

Combined DNA Index System (CODIS) Enhancements/ National Missing Persons DNA Program/ Federal Convicted Offender Program

CODIS blends forensic science and computer technology into a tool for linking violent crimes. It enables federal, state, and local forensic laboratories to exchange and compare DNA profiles electronically, thereby linking serial violent crimes to each other and to known offenders.

The Federal Convicted Offender Program has been fully integrated into CODIS. As of June 2006, CODIS has achieved 36,000 investigations aided, 8,000 offender hits and 3,500 forensic hits.

The National Missing Person DNA Database stores the mtDNA profiles in the Combined DNA Index System Missing Person (CODISMP) software. In Fiscal Year 2004, 199 cases were reported out and 283 cases were submitted to the National Missing Person DNA Database Program for analysis. Nationally, there were 21 cases where a match was made between the unidentified human remains and a biological relative of a missing person.

Latent Fingerprint Improvements

As a result of the misidentification of a latent print in the Madrid train bombing investigation in 2004, a number of critical reviews of the operations of the three Latent Print Units (LPUs) were conducted. One of these reviews consisted of an internal review by eight teams of experienced forensic examiners and scientists in the FBI Laboratory and outside experts. The internal review resulted in a large number of recommended changes which were approved by the FBI Laboratory in April 2005. Teams within the LPUs were established to develop new policies and procedures to implement the numerous recommendations, many of which have been completed. We have established Standard Operating Procedures (SOPs) pertaining to friction ridge analysis, Integrated Automated Fingerprint Identification System (IAFIS), and digital imaging, including minimum evidence requirements. All LPU personnel have received training in analysis methods and new SOPs. We