Testimony of Maureen A. Baginski
Executive Assistant Director – Intelligence
Federal Bureau of Investigation

Concerning Information Sharing
Under Subsections 203(b) and (d) of the USA Patriot Act

before the
Subcommittee on Crime, Terrorism, and Homeland Security
Committee on the Judiciary
United States House of Representatives

April 19, 2005

Good morning Mr. Chairman and Members of the Subcommittee. I am pleased to be here today with Barry Sabin, Chief of the Counterterrorism Section, Department of Justice Criminal Division to talk with you about the ways in which the USA Patriot Act has assisted the FBI with its information-sharing efforts. I will address the overall benefits of the information sharing provisions of the Act, including: the relevant amendments to the Foreign Intelligence Surveillance Act; Section 203(b), which authorizes the sharing of foreign intelligence information obtained in a Title III electronic surveillance with other federal officials, including intelligence officers, DHS/DOD/ICE officials, and national security officials; and Section 203(d), which specifically authorizes the sharing of foreign intelligence information collected in a criminal investigation with intelligence officials.

It is important to place the information sharing provisions of the USA Patriot Act in the context of subsequent Congressional action formalizing the FBI Intelligence Directorate in 2004. The Statement of Managers accompanying the Conference Report on H.R. 4818, Consolidated Appropriations Act, 2005 (House of Representatives – November 19, 2004), states:

> "...the conference agreement adopts the House report language directing the FBI to create a new Directorate of Intelligence....The need for effective intelligence capabilities cuts across all FBI programs including the counterterrorism, counterintelligence, criminal and cyber crime programs. This new directorate will ensure that intelligence is shared across these programs, eliminate information stove-piping, and allow the FBI to quickly adapt as threats change.... It shall also work to improve the FBI's capability to share intelligence, not only within the Bureau and the Intelligence Community, but also with State and local law enforcement."

I am here today to express to you how crucial renewal of the USA Patriot Act provisions related to information and intelligence sharing is to fulfilling the responsibilities of the FBI's new Directorate of Intelligence as envisioned by Congress.

There are two components to this subject: first, the issue of collecting intelligence and the legal authorities and policies that govern that collection; and second, how that information is actually shared once it is collected. I will address both in turn.

I realize that the collection authorities granted under the Patriot Act are of concern to many individuals and organizations. In that regard I want to say two things.

First, the FBI is committed to carrying out its mission in accordance with the protections provided by the Constitution. FBI agents are trained to understand and appreciate that the responsibility to respect and protect the law is the basis for their authority to enforce it. Respect for Constitutional liberties is not optional, it is mandatory for all FBI employees. The FBI could not be effective -- and would not exist -- without it.

Second, the FBI's authority to collect information is very clearly laid out in law and is directed by the Attorney General – the chief law enforcement officer for the United States. Intelligence collection is only done in accordance with the intelligence priorities set by the President, and is guided at every step by procedures mandated by the Attorney General. As soon as an international terrorism intelligence or counterintelligence case is opened, both Headquarters and the Department of Justice are notified. We are subject to and follow Attorney General's guidelines and procedures for FBI National Security Investigations and Foreign Intelligence Collection (NSIG); and all terrorism-related cases are subject to in-progress review by the Department of Justice (DOJ) Office of Intelligence Policy and Review, the DOJ Criminal Division, and local offices of U.S. Attorneys. We report annually to the Department of Justice on the progress of intelligence cases. The FBI's collection authorities are also controlled by the Federal Courts. Under the USA Patriot Act, a federal judge must still approve search warrants and wiretaps for counterintelligence and counterterrorism investigations and Agents must establish probable cause in order to obtain a FISA warrant. The FBI only collects and disseminates intelligence under guidelines designed specifically to protect the privacy of United States persons, and we are committed to using our authorities and resources responsibly.

After information is legally collected, the issue of how we pool that information arises. Effective intelligence requires skilled analysis and dissemination to meet the requirements of customers inside and outside the FBI. My job as the FBI's Executive Assistant Director for Intelligence is to manage the entire intelligence cycle to ensure that the FBI has the collection, reporting, analysis and dissemination capability it needs to protect the country. Information sharing is vital to that capability.

Effective FBI intelligence capabilities depend, first of all, on the integration of our intelligence collection and criminal investigative operations. During hearings on the 9/11 attacks, Congress heard testimony about meetings between the CIA and FBI where it was unclear what information on a hijacker could be legally shared under the widely-misunderstood set of rules and laws that was known as "the Wall." This wall extended into the FBI itself. Agents pursuing cases involving the Foreign Intelligence Surveillance Act (FISA) could not readily share information with agents or prosecutors working

criminal investigations. And the wall worked both ways – without FISA-derived information agents or prosecutors involved in a criminal case might not have any way of knowing what information from the criminal investigation might be useful to an agent working on a parallel international terrorism or counterintelligence investigation. Although there was some legal capability to share information, the law was complex and as a result, agents often erred on the side of caution and refrained from sharing the information. In addition, the wall functioned to discourage criminal and intelligence investigators from talking about their cases, such that investigators on either side might have no idea what might be useful to share with those on the other side of wall.

The Patriot Act tore down those legal walls between FISA-related intelligence and criminal investigations. Law enforcement and intelligence agents were able to coordinate terrorism investigations without fear of running afoul of the law as then interpreted.

Patriot Act Section 203(b) authorizes the sharing of foreign intelligence information obtained in a Title III electronic surveillance with other federal officials, including intelligence officers, DHS/DOD/ICE officials, and national security officials. If Section 203(b) were allowed to expire, FBI Agents would be allowed to share certain foreign intelligence information collected through criminal investigative wiretaps with foreign intelligence services, such as MI-5, but would arguably not be allowed to share that same information with the CIA. This result would be inconsistent with the spirit of the recently enacted Intelligence Reform and Terrorism Prevention Act of 2004, which included many provisions designed to enhance information sharing within the federal government.

An example of information sharing now permitted by section 203 of the USA PATRIOT Act takes place in the National Counterterrorism Center (NCTC) (formerly the Terrorist Threat Integration Center). The NCTC receives foreign intelligence information lawfully collected by its member entities, which includes international terrorism information collected by the law enforcement community. Information provided to NCTC pursuant to section 203 of the PATRIOT act is used in three crucial NCTC missions: the production of all-source terrorism analysis, updating the database used by other federal entities to prevent known or suspected terrorists from entering U.S. borders, and to ensure that agencies, as appropriate, have access to and receive all-source intelligence needed to execute their counterterrorism plans or perform independent, alternative analysis. The FBI, one of the NCTC's key members, relies upon section 203(d) of the USA PATRIOT Act to provide information related to international terrorism to NCTC analysts including intelligence, protective, immigration, national defense, national security, and other information related to international terrorism (a subset of foreign intelligence and counterintelligence information) obtained as part of FBI criminal investigations. In particular, section 203(d) authorizes law enforcement officers to disclose foreign intelligence or counterintelligence information to various federal officials, notwithstanding any other legal restriction. Without section 203(d), access to such FBI information by non-FBI personnel at NCTC could put us back to the pre 9-11 days of uncertainty about information sharing authorities. A decision by this Congress to

allow section 203(d) to sunset would send the message that full information sharing is discouraged and law enforcement and intelligence officials will once again be left with a complex legal regime and err on the side of caution and refrain from sharing terrorism information.

Furthermore, section 203 of the PATRIOT Act facilitates the NCTC's ability to provide strategic analysis to policy makers and actionable leads to officers within the FBI and the Intelligence Community (including components of the Department of Homeland Security (DHS)), transcending traditional government boundaries.

The NCTC estimates that the number of known or appropriately suspected terrorists intercepted at borders of the United States, based on FBI reporting alone, has increased due to the information sharing provisions of the USA PATRIOT Act. The NCTC maintains TIPOFF, an up-to-date database of known and appropriately suspected terrorists. The NCTC relies upon various agencies, which provide terrorist identity information on an on-going basis. Much of the terrorist identities information the NCTC receives from the FBI is collected in the course of criminal investigations and is shared pursuant to section 203.

Tearing down the wall between criminal and intelligence investigations actually enabled the FBI to conduct intelligence analysis and to integrate intelligence analysis into the Bureau. Our Intelligence Program now crosses all investigative programs – Criminal, Cyber, Counterterrorism, and Counterintelligence. And the Directorate of Intelligence is able to leverage the core strengths of the law enforcement culture – with its attention to the pedigree of sources and fact-based analysis – while ensuring no walls exist between collectors, analysts, and those who must act upon intelligence information to keep our nation safe. As FBI Director Mueller said in a speech to the American Civil Liberties Union (ACLU) in 2003: "Critical to preventing future terrorist attacks is improving our intelligence capabilities so that we can increase the most important aspect of terrorist intelligence information – its predictive value....The global aspect of terrorism creates an even greater need for the FBI to integrate its intelligence program and criminal operations to prevent attacks."

Facing today's threats, it makes no sense not to share information that has been legally collected with those who have a need for it and can maintain proper security and privacy safeguards.

Experience has taught the FBI that there are no neat dividing lines that distinguish criminal, terrorist, and foreign intelligence activity. Criminal, terrorist, and foreign intelligence organizations and activities are often interrelated or interdependent. FBI files are full of examples of investigations where information sharing between counterterrorism, counterintelligence and criminal intelligence efforts and investigations was essential to the FBI's ability to protect the United States from terrorists, foreign intelligence activity and criminal activity. Some cases that start out as criminal cases become counterterrorism cases. Some cases that start out as counterintelligence cases become criminal cases. Sometimes the FBI will initiate parallel criminal and

counterterrorism or counterintelligence cases to maximize the FBI's ability to adequately identify, investigate and address a variety of threats to the United States while protecting vulnerable sources and methods. The success of these cases in providing accurate intelligence threat assessments as well as arrests and convictions is entirely dependent on the free flow of information between the respective investigations, investigators and analysts.

Ongoing criminal investigations of transnational criminal enterprises involved in counterfeit goods, drug/weapons trafficking, money laundering and other criminal activity depend on close coordination and information sharing with the FBI's Counterterrorism and Counterintelligence Programs, as well as with other agencies in the intelligence community, when intelligence is developed which connects these criminal enterprises to terrorism, the material support of terrorism or state sponsored intelligence activity.

As an example of benefits from sharing intelligence from such a case, information from a criminal Title III surveillance and criminal investigation was passed to FBI Counterterrorism investigators and intelligence community partners, because the subject of the criminal case had previously been targeted by other agencies. Information sharing permitted the agencies to pool their information and resources to uncover the interplay of criminal and foreign intelligence activity.

As an example of sharing from a terrorism intelligence case, a terrorism investigation initiated in Minneapolis was subsequently transferred to San Diego and converted to a criminal case. The investigation focused on a group of Pakistan-based individuals who were involved in arms trafficking, the production and distribution of multi-ton quantities of hashish and heroin, and the discussion of an exchange of a large quantity of drugs for four stinger anti-aircraft missiles to be used by Al Qaeda in Afghanistan. The operation resulted in the arrest, indictment and subsequent deportation of the subjects, Syed Mustajab Shah, Muhammed Afridi, and Ilyas Ali, from Hong Kong to San Diego to face drug charges and charges of providing material support to Al Qaeda. In this case the benefits of immediate disruption by arrest outweighed the need for long-term intelligence coverage of the conspirators.

Another example came in the aftermath of the September 11th attacks. A reliable intelligence asset identified a naturalized U.S. citizen as a leader among a group of Islamic extremists residing in the U.S. The subject's extremist views, his affiliations with other terrorism subjects, and his heavy involvement in the stock market increased the potential that he was a possible financier and material supporter of terrorist activities. Early in the criminal investigation it was confirmed that the subject had developed a complex scheme to defraud multiple brokerage firms of large amounts of money. The subject was arrested and pled guilty to wire fraud. The close interaction between the criminal and intelligence cases was critical both to the successful arrest of the subject before he left the country and to the eventual outcome of the case. Once again, intelligence led to an arrest that was determined to be the most effective means to disrupt a potential terrorist threat.

Criminal enterprises are also frequently involved in, allied with, or otherwise rely on smuggling operations that do not respect jurisdictional lines between types of investigations or intelligence. Alien smugglers frequently use the same routes used by drug and contraband smugglers and do not limit their smuggling to aliens – they will smuggle anything or anyone for the right price. Terrorists can take advantage of these smuggling routes and enterprises to enter the U.S. and are willing to pay top dollar to smugglers. Intelligence developed in these cases also frequently identifies corrupt U.S. and foreign officials who facilitate smuggling activities. Current intelligence, based on information sharing between criminal, counterterrorism, and counterintelligence efforts, has identified smugglers who provide false travel documents to special interest aliens, deal with corrupt foreign officials, and financially support extremist organizations, as well as illegitimate and quasi-legitimate business operators in the United States, who not only use the services of illegal aliens, but are also actively involved in smuggling as well. These transnational criminal enterprises require global intelligence coverage, domestic as well as foreign, that transcends out-dated divisions between national security and criminal law enforcement.

Obviously, considering the cases I've just described, the information sharing provisions are overwhelmingly heralded by FBI Field Offices as the most important provisions in the USA Patriot Act. The ability to share critical information has significantly altered the entire manner in which terrorism and criminal investigations are conducted, allowing for a much more coordinated and effective approach than prior to the USA Patriot Act. Specifically, the Field Offices note that these provisions enable case agents to involve other agencies in investigations, resulting in a style of teamwork that enables more effective and responsive investigations, improves the utilization of resources allowing a better focus on the case, allows for follow-up investigations by other agencies when the criminal subject leaves the U.S., and helps prevent the compromise of foreign intelligence investigations.

From the perspective of the Directorate of Intelligence, the USA Patriot Act information sharing provisions are critical to the effectiveness of the Directorate's Field Intelligence Groups (FIGs) and to the integration of Directorate of Intelligence elements that are embedded in each of our headquarters investigative divisions. As authorized by the Congress, the Directorate now has a Field Intelligence Group in each field office that brings together the intelligence from criminal, counterterrorism, counterintelligence, and cyber investigations. The FIGs also include our language analysts who provide vital support to the full range of FBI investigations and intelligence collection. At headquarters, the Directorate manages intelligence analysis, in coordination with other elements of the intelligence community, to support both national security and crininal law enforcement requirements. Allowing the information sharing provisions of the USA Patriot Act to sunset would re-introduce barriers that would make intelligence sharing more difficult.

The Intelligence Reform Act directs the President to "create an information sharing environment for the sharing of terrorism information in a manner consistent with

national security and with applicable legal standards." It also directs the President to incorporate "protections for individuals' privacy and civil liberties," and further, to incorporate "strong mechanisms to enhance accountability and facilitate oversight, including audits, authentication, and access controls." The Intelligence Reform Act directs the DNI to implement those provisions and provides the DNI with a privacy and civil liberties officer to ensure implementation. The FBI has already implemented Executive Order 12333 in both our privacy systems and in the dissemination of information from our intelligence databases.

Specifically, we use a Privacy Impact Assessment (PIA) process to evaluate privacy in major record systems prior to system implementation. The PIA process requires that the system sponsor/developer conduct a thorough, written analysis of the impact on privacy that will result from the creation of a proposed system prior to the system's implementation. We assess both impacts attributable solely to the proposed system and the cumulative impacts arising from the proposed system's interface with existing systems. The PIA provides senior FBI management officials with a systemic assessment of a major new system's impact on privacy before the system becomes operational. The FBI PIA process includes a review of major systems by the FBI Privacy Council, a group composed of representatives from several FBI divisions, as well as an FBI Senior Privacy Official.

In summary, the information sharing provisions of the USA Patriot Act are vital to our national security. Allowing these provisions to sunset would be inconsistent with the spirit of the recently enacted Intelligence Reform and Terrorism Prevention Act of 2004, which included many provisions designed to enhance information sharing within the federal government. Provisions of the USA Patriot Act are critical to implementing the Congressional mandate for an "information sharing environment." Section 203(b) of the USA Patriot Act specifically authorizes the sharing of foreign intelligence information obtained in a Title III electronic surveillance with other federal officials, including intelligence officers and national security officials, such as DHS and DOD officials. Section 203(d) specifically authorizes the sharing of foreign intelligence information collected in a criminal investigation with intelligence officials. Allowing either of these provisions to sunset could seriously damage our information sharing and coordination efforts with the CIA, other intelligence agencies, and even internally between criminal and intelligence investigations.

Mr. Chairman and Members of the Subcommittee – thank you for your time and for your continued support of the FBI's information sharing efforts. I am happy to answer any questions.