Department of Justice

STATEMENT

OF

LANNY A. BREUER
ASSISTANT ATTORNEY GENERAL
CRIMINAL DIVISION

BEFORE THE

SUBCOMMITTEE ON CRIME AND TERRORISM
COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

AT A HEARING ENTITLED

"COMBATING INTERNATIONAL ORGANIZED CRIME: EVALUATING CURRENT AUTHORITIES, TOOLS, AND RESOURCES"

PRESENTED

NOVEMBER 1, 2011

Statement of Lanny A. Breuer
Assistant Attorney General
Criminal Division
U.S. Department of Justice

Subcommittee on Crime and Terrorism
Committee on the Judiciary
United States Senate

"Combating International Organized Crime: Evaluating Current Authorities, Tools, and Resources"
November 1, 2011

I. INTRODUCTION

Mr. Chairman, Senator Kyl, and distinguished Members of the Committee: Thank you for inviting me to speak with you this morning about the threat posed by transnational organized crime, the efforts of the Department of Justice to address the threat, and steps Congress can take that will assist in these efforts. I am honored to appear before you on behalf of the Department of Justice, along with my colleagues from the Departments of Treasury and Homeland Security.

The fight against transnational organized crime is one of the highest enforcement priorities of the Department of Justice and the Administration. Together with the United States Attorneys' Offices and our many law enforcement partners, the Criminal Division, whose fine lawyers and staff I am privileged to lead, investigates and prosecutes cases involving transnational organized crime all over the country, indeed, all over the world.

Transnational organized crime refers to self-perpetuating associations of individuals who operate transnationally for the purpose of obtaining power, influence, or commercial gains, wholly or in part by illegal means. These organizations promote and protect their activities through a pattern of violence and corruption, including by insinuating themselves into the political process and becoming alternate providers of governance, security, and livelihoods to win popular support. In the process, transnational organized criminals are often assisted by willing facilitators, including lawyers, bankers, and business owners, who exploit their professional legitimacy to perpetuate and disguise illegal activity and profits.

The convergence of threats posed by these groups is significant and growing. Last year, the National Intelligence Council issued an unclassified report identifying five key threats that transnational organized crime poses to United States national security:

1. Penetration of State Institutions. Transnational organized crime's penetration of governments is subverting the rule of law, democratic institutions, and transparent business practices. The growing reach of transnational organized criminal networks is

pushing them to seek strategic alliances with state leaders and foreign intelligence services, threatening stability and undermining free markets.

2. Threat to the U.S. and World Economy. Transnational organized crime is increasing its subversion of legitimate financial and commercial markets, threatening U.S. economic interests and raising the risk of significant damage to the world financial system.

3. Growing Cybercrime Threat. Transnational organized criminal networks are becoming increasingly involved in cybercrime, which costs consumers billions of dollars annually, creates risks to sensitive corporate and government computer networks, and undermines worldwide confidence in the international financial system.

4. Threatening Crime-Terror Nexus. Terrorists and insurgents are increasingly turning to crime to generate funding and acquire logistical support.

5. Expansion of Drug Trafficking. Despite demonstrable counterdrug successes in recent years, illicit drugs remain a serious threat to the health, safety, security, and financial well-being of U.S. citizens.

Responding to this assessment, in July the Administration released its Strategy to Combat Transnational Organized Crime ("TOC Strategy"), which set forth a whole-of-government response to the enumerated threats. At the announcement of the TOC Strategy, Attorney General Eric Holder noted:

> Today's criminal organizations are increasingly sophisticated. They know no borders. They threaten the stability of our financial system and the promise of a competitive marketplace. And their operations are putting far too many American businesses, government institutions, consumers, and citizens at risk.

The TOC Strategy outlines several strategic objectives at the heart of the Department's efforts to address this threat:

- the protection of Americans from the harm, violence, and exploitation of transnational criminal networks;

- breaking the economic power of transnational criminal networks and protecting strategic markets and the U.S. financial system from penetration and abuse by transnational criminal organizations; and

- defeating transnational criminal networks that pose the greatest threat to national security by targeting their infrastructures, depriving them of their enabling means, and preventing the criminal facilitation of terrorist activities.

The strategy also recognizes that some intellectual property rights (IPR) and cyber crimes merit particular attention, as well as the need to strengthen and safeguard our financial system:

> [S]ome TOC activity is inherently harder to detect and deter. The United States will place special emphasis on IPR violations and cybercrimes due to their particular impact on the economy and consumer health and safety. The United States remains intent on improving the transparency of the international financial system, including an effort to expose vulnerabilities that could be exploited by terrorist and other illicit financial networks. At the same time, the United States will enhance and apply our financial tools and sanctions more effectively to close those vulnerabilities, [and] disrupt and dismantle illicit financial networks.

The Department of Justice is committed to the fight against transnational organized crime and we have enjoyed certain successes to date. However, serious challenges remain, and additional tools are needed. As part of the TOC Strategy, the Administration has proposed a number of important legislative improvements, which the Department believes could assist us and our law enforcement partners in meeting these challenges and addressing the identified threats.

II. CURRENT SUCCESSES IN COMBATING TRANSNATIONAL ORGANIZED CRIME

The Department has made great strides in attacking transnational organized crime groups, particularly those with some physical presence or foothold in the United States. We have prosecuted groups involved in narcotics and narco-terrorism, kidnapping and extortion, and health care and other identify fraud crimes alike. Below are several key examples:

- Joint Colombian-United States Drug Trafficking Investigation: On September 2, 2011, the U.S. Attorney's Office for the Southern District of Florida announced that 34 individuals were charged in five separate indictments in an operation that targeted a Drug Trafficking Organization (DTO) based in Bogota, Colombia that utilized U.S. registered aircraft to transport thousands of kilograms of cocaine from South America, to clandestine airstrips in Central America and the Caribbean region. The drug trafficking organization is alleged to have purchased U.S. registered aircraft using nominees, who in turn submitted false documentation to the Federal Aviation Administration (FAA) to hide the identities of the South American drug traffickers who were purchasing the planes. The Colombian-based DTO, which arranged for the aircraft to depart from South America, allegedly had ties to drug trafficking organizations in Mexico. During the course of the investigation, law enforcement seized 1300 kilograms of cocaine, $1.6 million in U.S. currency, and eight U.S. registered aircraft. The case is being prosecuted by a special unit within the Southern District of Florida that was established in February 2011, to prosecute the violent Bandas Criminales (BACRIM) drug trafficking groups in Colombia.

- Armenian Health Care Fraud: In October 2010, the Department announced charges against 73 members and associates of an Armenian-American organized crime group, with ties abroad, in five states (California, Georgia, New Mexico, New York and Ohio) for various health care fraud-related crimes involving more than $163 million in fraudulent billing. The defendants were charged with engaging in numerous frauds,

including sophisticated schemes to defraud Medicare and insurance companies by submitting fraudulent bills for medically unnecessary treatments or treatments that were never performed. As part of this prosecution, the defendant Armen Kazarian became the first "Vor" or "Thief-in-Law," convicted of racketeering in the United States.[1]

- International Computer Hacking: In November 2009, charges were filed based on a successful FBI investigation into a sophisticated international computer hacking ring involving defendants from Estonia, Russia, and Moldova. Various defendants were charged in the Northern District of Georgia with hacking into a computer network operated by a credit card processing company and using sophisticated techniques to compromise the data encryption used to protect customer data on payroll debit cards. Ultimately, counterfeit devices were employed to withdraw over $9 million from more than 2,100 ATMs in at least 280 cities worldwide, including cities in the United States, Russia, Ukraine, Estonia, Italy, Hong Kong, Japan, and Canada. Remarkably, this loss occurred within a span of less than 12 hours. Through this investigation, the FBI uncovered a previously undetected hacking technique that compromised the bank's encryption system. This information was disseminated throughout the banking sector to prevent further losses. Five Estonian defendants have been arrested and charged in Estonia. One of those defendants was extradited to the United States. Additionally, one defendant in the United States and two defendants residing in Hong Kong were arrested for their involvement in this criminal enterprise.

- Armenian Power Takedown: In February 2011, federal prosecutors from the United States Attorney's Office for the Central District of California, the Southern District of Florida and the Criminal Division announced charges against more than 100 members and associates of Eurasian organized crime groups, in six indictments, in four cities. The arrests included more than 80 defendants from the Armenian Power group, who were charged with a wide variety of violent and fraud-related crimes. The alleged crimes included kidnapping, extortion, assault, witness intimidation, bank fraud, credit card fraud and drug distribution. AP's membership consists primarily of individuals whose heritage goes back to Armenia and other Eastern Bloc countries. AP is an international organized crime group that started as a street gang in East Hollywood, California in the 1980s.

- Operation Whirling Dervish: In July 2011, the Department announced charges resulting from a DEA narco-terrorism undercover operation, charging three defendants with conspiring to provide various forms of support to Hizballah, the PKK, and Pejak. Two defendants were arrested in Bucharest, Romania, where they were detained pending extradition to the United States; the third was arrested in the Republic of the Maldives. This investigation was supported by Romanian authorities who identified Kurdish PKK members that were selling heroin to support their terrorist organization. It also identified

[1] A "vor" (translated as "Thief-in-Law" refers to a member of a select group of high-level criminals from Russia and counties that had been part of the former Soviet Union, including Armenia. "Vors" offer prestige and protection to criminal organizations in return for a share of the criminal earnings, and use their position of authority to resolve disputes among criminals.

Iranian Pejak elements that were utilizing the drug trade to finance operations and Hizballah elements that were attempting to purchase military-grade weaponry. This investigation is continuing.

- Eastern European Money Laundering: In June 2011, a joint prosecution between the Division's Computer Crime and Intellectual Property Section of the Criminal Division and the U.S. Attorney's Offices in Chicago and Washington, D.C., resulted in a Romanian man being sentenced to 48 months imprisonment in the United States for his role in an international money-laundering scheme involving the creation of fraudulent online auctions. In a similar case handled by the Criminal Division's Organized Crime and Gang Section, a Bulgarian man was sentenced this September to 64 months imprisonment for his role in an auction scheme, which appears to have been orchestrated by a transnational criminal group based in Eastern Europe. Another individual, a Romanian citizen, was sentenced to 24 months imprisonment for his role in the same conspiracy, also in September 2011. According to court documents, in less than one year, the scheme netted more than $1.4 million from U.S. victims.

As is clear from the examples cited above, a key component of our transnational organized crime strategy has been forging successful and strategic partnerships with foreign law enforcement authorities. The example of Romania is instructive. It is estimated that approximately one-third of so-called "phishing" attacks targeting United States citizens originate in Romania, and we have worked closely with authorities there to identify and prosecute those involved.[2] As an important first step, several law enforcement agencies, including the Federal Bureau of Investigation, the United States Secret Service and the Drug Enforcement Administration, have employees stationed in Romania, who work side by side with Romanian law enforcement in an effort to target cyber-criminals and other organized crime. The results have been significant. Earlier this year, joint United States-Romanian investigations resulted in the arrest of over 100 organized crime related cyber-criminals in our two countries. Those arrests involved various schemes involving the fake sales of merchandise, including cars and boats, over the Internet to thousands of victims in the United States and elsewhere.

Just last month, I traveled to Romania and, in meeting with United States and Romanian law enforcement, I observed first-hand how closely our two nations are collaborating. Through joint cooperation efforts with our foreign counterparts and by deploying our resources in innovative ways, we have succeeded in disrupting and dismantling various criminal syndicates attacking United States citizens and property.

Another important innovation critical to our efforts has been the development of the International Organized Crime Intelligence and Operations Center, or IOC-2, here in the Department of Justice. Building on our successful counter-narcotics work, IOC-2 brings together nine federal law enforcement agencies in a powerful center to share data and intelligence, both domestically and internationally, on organized crime investigations. IOC-2 greatly expands our abilities to spot patterns and coordinate investigations against transnational

[2] "Phishing" refers to an email fraud method in which the perpetrator sends out legitimate-looking email in an attempt to gather personal and financial information from recipients.

organized crime networks. IOC-2 also aids our attempts to identify forfeitable assets associated with international criminal activities and promote seizure and forfeiture judgments.

III. CHALLENGES TO GREATER SUCCESS

Our work on transnational organized crime enforcement is far from over. While the threat is clear, the obstacles to successfully investigating, prosecuting and dismantling these networks are numerous. Transnational organized crime groups and the offenses they commit present significant challenges. As a point of comparison, it has been well documented that domestic organized crime syndicates employ tactics that create many roadblocks for law enforcement: layers of secrecy, corruption of officials, and fear and intimidation that silence witnesses. Despite these challenges, over the years, Congress and the Department of Justice have developed methods of attacking domestic organized crime to the point where our record of achievements is one of the federal government's great success stories. Transnational organized crime poses an additional dimension of challenges: while the effects are felt here in the United States, the perpetrators, witnesses and evidence reside abroad, often in jurisdictions unable or unwilling to cooperate with our investigative efforts.

Take a few simple examples. Organized cyber criminals direct cyber attacks from abroad that target United States citizens and steal their identities for the purpose of raiding bank accounts or placing fraudulent credit card purchases. Other organized criminals commit crimes abroad and launder and maintain funds in the United States, without ever traveling to our shores, and sometimes through the use of U.S. shell corporations.

In each instance, the investigation and prosecutions of these organizations and crimes pose significant challenges. At a minimum, pursuing an investigation abroad is often time consuming and delays can be significant and undermine an investigation. Tracking down criminals abroad often requires the cooperation of foreign law enforcement agencies and even if we locate our targets, many of the investigative tools for gathering evidence are not available to us in an international context. In some countries, we cannot employ Title III wiretaps against the perpetrators, nor can we, in many cases, send an undercover agent to gather incriminating statements. The country's law enforcement agencies may not have the level of training or the necessary technology to implement the investigative steps, even if they are authorized.

Arresting lower level members of the organization and persuading them to cooperate against higher level bosses is also extremely difficult and may require the approval and cooperation of foreign authorities, as well as navigating various domestic immigration and other laws. Other countries have domestic laws which ban the extradition of their own citizens to foreign countries for prosecution. In such instances, the only option may be for the foreign government to prosecute the target under their domestic laws, and often the associated penalties are little more than a "slap on the wrist," particularly in cybercrime cases. Still other targeted organized crime groups may have so penetrated the country's law enforcement entities or political leadership that the country will refuse to answer our request for assistance.

These concerns are not hypothetical. The prosecution, or the attempted prosecution, of Semion Mogilevich makes this clear. Mogilevich is a powerful Russian organized crime figure

and the head of an international criminal enterprise engaged in activities designed to penetrate and corrupt strategic sectors world-wide. He and his co-conspirators were indicted by the U.S. Attorney's Office for the Eastern District of Pennsylvania in 2003 on racketeering, securities fraud and money laundering charges, yet remain at liberty. At the heart of the charged crimes was a sophisticated multi-million dollar scheme responsible for defrauding thousands of investors in the United States, Canada and abroad in the stock of a public company that was headquartered in the United States. The indictment alleges that, while residing in Eastern Europe, Mogilevich funded and controlled a criminal enterprise, comprised of individuals and companies in over twenty countries throughout the world, including corrupt accountants and auditors, and numerous United States shell companies which were used to conceal their involvement and to launder proceeds from the scheme. Despite committing crimes here, Mogilevich remains outside our reach and is believed to currently be residing in Moscow, Russia. He is currently on the *FBI's Ten Most Wanted Fugitives List*.

Those transnational criminal networks involved in cyber crimes pose even further barriers to prosecution. The technology revolution has facilitated cyber crime, enabling those involved to access and exploit the personal information of others. Today's criminals can remotely access the computer systems of government agencies, universities, merchants, financial institutions, credit card companies, and data processors from thousands of miles and many international borders away to steal large volumes of personal information – including personal financial information.

Finally, the ability of transnational criminal organizations to generate vast sums of money is both their strength and their weakness. Criminal organizations are businesses, and like any business profit is their primary motivation. The wealth generated by today's drug cartels and other international criminal networks enables some of the worst criminal elements to operate with impunity while wreaking havoc on individuals and institutions around the world. Generating proceeds often is only the first step –criminals then launder their proceeds, often using our financial system to move or hide their assets and often with the help of third parties located in the United States. Indeed, international criminal organizations increasingly rely on these third parties and on the use of domestic shell corporations to mask crimes and launder proceeds under the guise of a seemingly legitimate corporate structure. We can use our asset forfeiture laws to take the assets away from the criminal organizations and dismantle their financial infrastructures but, as discussed below, the existing law needs to be modernized.

IV. LEGISLATION

There are important steps we can take to better address extraterritorial threats and the increasingly global reach of transnational criminal organizations. The Department of Justice together with our partners have developed a package of legislative proposals to ensure that federal law keeps up with the rapid evolution of organized criminal activity. We need changes to our existing money laundering, asset forfeiture, narcotics and racketeering laws. Additional proposals recognize that in an increasingly global law enforcement environment, witness security and protection for foreign witnesses must also be available. And finally, stiffer penalties for certain crimes, such as intellectual property offenses, which are increasingly the focus of transnational organized crime, are also necessary. These proposals are outlined below.

A. Anti-Money Laundering and Forfeiture Laws

The TOC Strategy recognizes that criminals who commit their crimes overseas often launder and maintain their assets in the United States. Accordingly, a focal point of the Strategy is the Proceeds of Crime Act (POCA) a comprehensive money laundering and forfeiture proposal designed to address gaps in our current legal authority. Money laundering and forfeiture laws strike at the very core of transnational criminal organizations by preventing them from using our financial system to move and hide their money, and by depriving them of the profit and capital needed to operate their enterprises.

POCA would update and clarify the current list of specified unlawful activities that are predicates for money laundering to include all domestic felonies except those specifically exempted, state felonies and federal misdemeanors that are included in the existing racketeering predicates, and any foreign crimes that would be felonies in the United States. The changes sought would also increase the scope and effect of anti-money laundering provisions in laws concerning promotional money laundering, bulk cash smuggling, tax evasion, and money laundering through informal value transfer systems, and would clarify the application of the law to commingled funds and aggregated transactions. Finally, the proposal also extends wiretap authority for money laundering offenses, and it extends the extraterritorial provision for money laundering to non-United States citizens where their extraterritorial acts in violation of 18 U.S.C. § 1956 cause an effect in the United States. These changes would fill in numerous gaps and omissions in our decades-old anti-money laundering laws and improve the ability to prosecute money launderers and to forfeit criminal proceeds and facilitating property.

POCA also seeks to update our civil forfeiture capabilities. Civil forfeiture is a particularly effective tool in this regard, as it enables prosecutors to forfeit the proceeds of crime even when criminal prosecutions of those involved are not possible. Thus fugitives, drug kingpins, and corrupt foreign officials not present in the United States cannot elude the reach of our enforcement entirely.

POCA would enhance the government's civil forfeiture authority in a number of important ways. It seeks to expand the scope of civil forfeiture authority to include "facilitating property," or property that enables crime to occur, for all money laundering predicates and broadens the categories of facilitating property that can be civilly forfeited in connection to drug offenses and alien smuggling and harboring. To better attack the financial infrastructures of these organizations through more effective financial investigations, the proposal provides increased civil forfeiture, administrative, and foreign bank record subpoena authority. It also would enable the use of classified information in civil forfeiture cases, which is critical in going after transnational criminal organizations that threaten our national security.

Taken together, the changes will make our investigations and prosecutions against the financial operations of transnational organized crime groups much more effective. By taking their money, we take away these groups' reason to exist and ability to operate. We are committed to working with Congress to combat the use of shell companies to generate and move illicit

money by requiring that those who form entities in the United States disclose beneficial owner information.

B. Racketeering Provisions

Second, the Administration proposes to modernize our most powerful anti-organized crime statutes: the Racketeer Influenced and Corrupt Organizations Act, or RICO, and the Violent Crimes in Aid of Rackeetering statute, or VICAR. The proposed amendments to the RICO statute, 18 U.S.C. § 1961, *et seq.*, would clarify that RICO has extraterritorial application in cases where criminal enterprises operate at least in part in the United States, or where they commit any predicate acts in the United States, or where the charged pattern includes offenses that apply extraterritorially. Criminal organizations have expanded their activities to increase their power, influence, and wealth, availing themselves of new opportunities. The proposed legislation, therefore, expands the list of racketeering predicate crimes to include offenses that are prevalent in an increasingly interconnected world and engaged in by transnational organized crime groups, including economic espionage, computer fraud, aggravated identity theft, violations of the Foreign Corrupt Practices Act, health care fraud, illegal firearms trafficking, as well as a limited number of violations of foreign law.

These proposed changes are important to address a number of recurring issues in organized crime prosecutions. In a number of instances, the government has been unable to charge the members or associates of a criminal enterprise with RICO because the underlying criminal activities were not listed as predicates. The new predicates are intended to fill these gaps.

Amendments to the Violent Crimes in Aid of Racketeering (VICAR) statute, 18 U.S.C. § 1959, are also recommended, including a provision which would provide for extraterritorial application in certain situations such as when the underlying statute criminalizing the violent act in question applies extraterritorially or when any part of the violation occurs within the jurisdiction of the United States.

C. Witness Protection

The Administration is also proposing legislation that fosters international cooperation regarding the relocation of witnesses giving testimony in criminal cases, and relatives and other persons close to them. Relocation is sometimes the only way to protect the security of such persons, and enhancing our ability to cooperate with foreign governments in these situations will greatly improve our ability to mount multinational operations against high-priority transnational organized crime targets**.**

D. Extraterritorial Jurisdiction

The Administration proposes criminalizing conduct occurring on vessels or aircraft owned by the United States or a United States citizen, vessels registered under U.S. or state law, and aircraft registered under United States law if such vessels or aircraft are outside the jurisdiction of any particular state. In the absence of such expanded jurisdiction, the United

States would, for example, lack federal jurisdiction over a sex-trafficking offense committed on board a United States-registered vessel or aircraft located between two foreign countries. Our proposal would address an existing reservation on jurisdiction by the United States to the 2000 UN Transnational Organized Crime Convention, and in particular the supplementing Trafficking in Persons Protocol.

E. Intellectual Property Crimes

Intellectual property crime is a strong lure to transnational organized criminal enterprises, which have increasingly turned to counterfeiting and piracy as a relatively low risk high reward means to fund their other unlawful activities. The Administration is seeking to strengthen penalties involving particularly egregious intellectual property offenses. Specifically, as first recommended in the Administration's White Paper on Intellectual Property Enforcement Legislative Recommendations transmitted to Congress by the Intellectual Property Enforcement Coordinator, the Administration has proposed that Congress issue direct the United States Sentencing Commission to consider several sentencing enhancements for offenses committed in connection a variety of aggravated conduct, including when the IP crime is committed in furtherance of criminal activities of local, national, or international criminal enterprises or when it involves the conscious or reckless risk of death or serious bodily injury. Furthermore, it is imperative that defendants whose sale of infringing products for use in critical infrastructure, national defense, security, and law enforcement face significant criminal penalties, and the Administration is recommending that Congress direct the Sentencing Commission to consider an enhancement in this circumstance.

F. Narcotics

The Administration proposes to expand conspiracy liability when controlled substances are destined to the United States from a foreign country. Under our proposal, members of any conspiracy to distribute controlled substances will be subject to United States jurisdiction when at least one member of the conspiracy intends or knows that the drugs will be unlawfully imported into the United States. We are also recommending changes to sentencing policy for violations of the Narcotics Kingpin Designation Act. Such violations currently carry statutory penalties of up to 30 years' imprisonment and/or fines up to $5,000,000. Sentencing guidelines for these violations, however, do not yet exist. The Administration is recommending a congressional directive to the United States Sentencing Commission, proposed statutory language, and a proposed sentencing guideline to yield a sentencing range of 37 - 46 months for a first offender, absent adjustments or departures.

V. CONCLUSION

Transnational organized crime presents many new challenges for United States law enforcement. The investigations and prosecutions of transnational organized criminals groups are among the most difficult and complex cases in the Department. Even as we develop our cases and push the envelope of what our agents and prosecutors have tried in the past, the criminals continue to evolve rapidly, deploying new techniques and strategies to evade our nets and continue their illegal activities. It is important to ensure that federal agents and prosecutors are fully armed with the most comprehensive and up to date legislative and investigative tools to

carry this fight across the globe and attack the criminals where they live. Only in this way can we protect our citizens, corporations, and property from those who would take them from us.