Department of Justice

**STATEMENT**
**OF**
**J. PATRICK ROWAN**
**DEPUTY ASSISTANT ATTORNEY GENERAL**
**NATIONAL SECURITY DIVISION**
**DEPARTMENT OF JUSTICE**

**BEFORE THE**
**SUBCOMMITTEE ON CRIME, TERRORISM, AND HOMELAND SECURITY**
**COMMITTEE ON THE JUDICARY**
**HOUSE OF REPRESENTATIVES**

**CONCERNING**

**"ENFORCEMENT OF FEDERAL ESPIONAGE LAWS"**

**PRESENTED**

**JANUARY 29, 2008**

**Statement of**
**J. Patrick Rowan**
**Deputy Assistant Attorney General**
**National Security Division**
**U.S. Department of Justice**

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

**Concerning**
**"Enforcement of Federal Espionage Laws"**

**January 29, 2008**

Chairman Scott, Ranking Member Gohmert, and members of the Subcommittee:

It is my pleasure to appear before you today to discuss the National Security Division's enforcement of Federal espionage laws. As you know, the clandestine intelligence collection activities of foreign nations include not only traditional Cold War style efforts to obtain military secrets, but, increasingly, sophisticated operations to obtain trade secrets, intellectual property, and technologies controlled for export for national security reasons. Accordingly, these activities and others implicate a wide array of Federal criminal statutes. But no matter what form of espionage is being used, or which statutes are implicated, there is one common denominator: our national security is always at stake.

Unfortunately, espionage did not end with the end of the Cold War, and in fact, we have investigated espionage activities relating to more countries now than in the past. Recent cases have involved efforts to get information or technology to countries like China, Cuba, the Philippines, and South Korea, for example:

- Noshir Gowadia is a former design engineer from Northrop Corporation who has been charged in an 18-count superseding indictment in the District of Hawaii with espionage and export violations stemming from substantial defense related services he allegedly performed for the Peoples Republic of China. This includes his illegal sale of U.S. military technology secrets to China. Gowadia allegedly agreed to design, and later designed, a "low observable" cruise missile exhaust system nozzle capable of rendering the missile less susceptible to detection and interception. The case is set for trial in the District of Hawaii in October 2008.

- Carlos Alvarez, a psychology professor at Florida International University, admitted in a guilty plea in 2006 that he had worked for nearly 30 years as a

covert intelligence agent on behalf of the Cuban government. He was sentenced to 60 months imprisonment.

- Leandro Aragoncillo, an FBI analyst, pleaded guilty in 2006 to espionage and other charges, admitting that he took and transferred classified information, including national defense documents, to senior political and government officials of the Republic of the Philippines. He was sentenced to 10 years imprisonment.

- Robert C. Kim, a South Korean native who had become an American citizen and had worked as a computer specialist for the U.S. Navy, pleaded guilty in 1996 to conspiracy to commit espionage for South Korea. He admitted to having given secret Pentagon and State Department documents to a South Korean naval attache at the South Korean Embassy in Washington. He was sentenced to 9 years imprisonment.

- Brian Patrick Regan, a former Master Sergeant in the United States Air Force who worked as a signal specialist at the National Reconnaissance Office, was convicted in 2003 of offering to sell U.S. intelligence secrets to China and Iraq. He was sentenced to life imprisonment without parole.

Of great concern recently is the substantial and growing national security threat posed by illegal foreign acquisition of restricted U.S. military technology. On January 22nd the President issued an Export Control Directive to ensure that U.S. defense trade policies and practices better support the National Security Strategy of the United States. One key element of this White House directed effort is the establishment of a multi-agency working group to support the Department's export enforcement investigations. The National Security Division will play a key role in this effort. Strict enforcement of our country's export control laws is a critical tool in stemming this somewhat non-traditional espionage-related threat. The National Security Division launched a new initiative this past October to bolster our enforcement efforts on that front. I'll discuss that initiative in greater detail shortly, but in a general sense, the technology at the heart of the initiative includes U.S. military items, dual-use equipment, and other technical expertise or know-how, some of which have applications in Weapons of Mass Destruction. These materials are generally restricted and may not be exported without a license. China and Iran pose particular U.S. export control concerns, and recent prosecutions have highlighted illegal exports of stealth missile technology, military aircraft components, Naval warship data, night vision equipment, and other restricted technology destined for those countries. In one recent case, a former engineer with a U.S. Navy contractor was convicted by a jury in May 2007 of exporting sensitive defense technology to China. The individual, Chi Mak, had been given lists from co-conspirators in China that requested U.S. Naval research related to nuclear submarines and other information. Mak gathered technical data about the Navy's current and future warship technology and conspired to export this data to China. His four co-defendants all pleaded guilty. Mak is scheduled to be sentenced in March of this year.

In the National Security Division, we have a section aptly named the Counterespionage Section, where lawyers work on espionage and espionage-related enforcement efforts everyday.

The Counterespionage lawyers are in constant communication with the foreign counterintelligence personnel in the FBI and, indeed, the entire intelligence community. They evaluate pending counterintelligence investigations for potential prosecution and are highly experienced in dealing with sensitive sources and methods. Since espionage prosecutions often involve the possibility that classified information may be disclosed publicly, either as part of the defendant's defense or as part of the prosecution's case-in-chief, the lawyers in the Counterespionage Section also work extensively with the Classified Information Procedures Act, known as CIPA, which provides uniform procedures for dealing with classified information in open criminal proceedings.

As mentioned above, the Federal criminal code gives the government a variety of different tools to prosecute different types of espionage. Lawyers in the Counterespionage Section of the National Security Division deal with all of the espionage and espionage-related statutes regularly. The primary statutes concerning espionage include 18 U.S.C. § 793 and § 794. Generally speaking, Section 793 prohibits anyone from willfully communicating information relating to the national defense to any person not entitled to receive it. The term "information relating to the national defense" has been defined by case law to mean information that is closely held by the government, usually through proof that the information was classified. Section 793 also criminalizes the willful retention of national defense information, conspiracies to communicate or retain national defense information, and the negligent removal of national defense information from its proper place of custody. The maximum penalty under Section 793 is ten years imprisonment. Section 794 is more narrow than Section 793 because it criminalizes the communication of national defense information to foreign governments, where the communication of information is made with intent or reason to believe that the information is to be used to the injury of the United States, or to the advantage of any foreign nation. Violations of Section 794 can result in life imprisonment, or, if certain criteria are met, the death penalty can be imposed.

In addition to Sections 793 and 794, there are other relevant statutes that provide felony offenses for more particularized conduct. For example, 18 U.S.C. § 798 prohibits disclosing classified information concerning communications intelligence; 18 U.S.C. § 1030(a) criminalizes obtaining of classified information by accessing a computer without authorization; 50 U.S.C. § 421 prohibits the disclosure of the identity of a United States covert agent; 50 U.S.C. § 783 makes it unlawful for any government employee to disclose classified information to a foreign government and for any agent of a foreign government to receive classified information from a government employee; and 18 U.S.C. § 951 prohibits anyone from acting in the United States as an agent of a foreign government without first notifying the Attorney General. All of these offenses generally carry a maximum penalty of ten years imprisonment. In addition to these felonies, Title 18 U.S.C. § 1924 provides a misdemeanor offense for retaining classified information.

One point of note with respect to one of the statutes mentioned above,18 U.S.C. § 951, is that it has been used successfully in recent cases to prosecute individuals who had been affiliated with the Iraqi Intelligence Service under Saddam Hussein, and who had been sent to the United States to conduct activities on behalf of Hussein's government. One example of this is Khaled

Abdel-Latif Dumeisi, who was convicted in the Northern District of Illinois of violating § 951 for his activities spying on Iraqi dissidents in the United States for Saddam Hussein. On March 31, 2004, Dumeisi was sentenced to 46 months imprisonment.

The Dumeisi case also provides just one example of how electronic surveillance under the Foreign Intelligence Surveillance Act ("FISA") is a key tool in combating intelligence collection activities by foreign governments here in the United States. Dumeisi had previously been the subject of an FBI intelligence investigation for several years, which had included electronic surveillance under FISA . In 2003, when FBI agents were able to share that information from their investigation with prosecutors, the prosecutors were able to use it to build the case against Dumeisi. Electronic surveillance and physical searches under FISA are indispensable in espionage cases, which by their very nature usually involve clandestine activities that are difficult to detect.

As discussed earlier, export control laws are also critical tools for addressing the national security threat posed by sensitive U.S. technology getting into the wrong hands. These include:

- the Arms Export Control Act, 22 U.S.C. §§ 2751-2799, which prohibits the export of defense articles and services without first obtaining a license from the Department of State, and carries a penalty of up to 10 years imprisonment;

- the Export Administration Act of 1979, 50 U.S.C. App. §§ 2401-2420, which has lapsed and is therefore currently enforced through IEEPA, prohibits the export of certain "dual-use" goods and technology without first obtaining a license from the Department of Commerce, and carries a penalty of up to 5 or 10 years imprisonment depending on the violation;

- the International Emergency Economic Powers Act, 50 U.S.C. §§ 1701-1706, which authorizes restrictions or prohibitions on transactions (including comprehensive trade embargoes) involving particular countries, such as Iran, or specified individuals or entities, such as terrorists, and carries a penalty of up to 20 years imprisonment; and

- the Trading with the Enemy Act of 1917, 50 U.S.C. §§ App. 1-6, 7-39, 41-44, which authorizes prohibitions on nearly all transactions involving Cuba and on participation in transfers of certain strategic goods to North Korea, and carries a penalty of up to 10 years imprisonment.

The National Security Division's export enforcement initiative I described earlier is a major effort to ensure that prosecutors around the country have the training, tools, and support from other agencies that they need to bring cases under these statutes. The Department of Justice and the National Security Division are fully committed to the success of this important initiative. Steven Pelak, an 18-year veteran Federal prosecutor, has been appointed as the National Export Control Coordinator responsible for leading the efforts under the initiative. Mr. Pelak is creating multi-agency counter-proliferation task forces in U.S. Attorney's offices around

the country. These task forces are taking many of the concepts used in combating terrorism – namely, prevention, cooperation and coordination – and applying them to the efforts to prevent the illegal export of sensitive U.S. technology. The FBI, the Departments of State and Commerce, the Department of Homeland Security, the Defense Criminal Investigative Service, and others are all part of this effort. Training for prosecutors is of course an essential aspect of the initiative, since export prosecutions are by their very nature complex: they involve intricate laws, sensitive international issues, agencies with different authorities, and, often, classified information. Earlier this month, Mr. Pelak held a training symposium on export control for over 30 prosecutors from around the country at the National Advocacy Center. From the strides Mr. Pelak has already made in carrying out the National Security Division's export control initiative, we are confident that it will significantly bolster our country's export enforcement efforts.

Before I conclude I would be remiss if I did not point out that our efforts to disrupt clandestine intelligence activities of every form – from traditional spying to illegal exports of technology – have been enhanced by the establishment of the National Security Division within the Department of Justice, which brought the Counterespionage Section, the Counterterrorism Section, and the Office of Intelligence and Policy Review together in one Division. This Division was created by the Congress as part of the reauthorization of the Patriot Act in 2006, and we believe that it has already begun to pay dividends.

Thank you for the opportunity to appear before you and testify on the National Security Division's enforcement of Federal espionage laws. We look forward to working with the Committee to improve our enforcement capabilities in this important area.