April 14, 2004

Statement for the Record of
John O. Brennan
Director, Terrorist Threat Integration Center

On
Law Enforcement and the Intelligence Community

Before the
National Commission on Terrorist Attacks Upon the United States
Washington, D.C.

Good afternoon, Chairman Kean, Vice Chairman Hamilton, and Members of the National Commission on Terrorist Attacks Upon the United States.

I welcome the opportunity to join my colleagues from the Federal Bureau of Investigation (FBI), the Central Intelligence Agency (CIA), and the Department of Homeland Security (DHS) to discuss intelligence and law enforcement efforts to prevent terrorist attacks against U.S. interests. It is also a privilege for me to represent the many men and women from throughout the Government who have joined forces in an unprecedented manner in the new Terrorist Threat Integration Center (TTIC).

As members of the Commission and the American public well know, the scourge of international terrorism poses a serious threat to U.S. interests, both at home and abroad. Since the devastating attacks of September 11, 2001, hundreds of innocent lives have been lost in terrorist attacks in Tunisia, the Philippines, Saudi Arabia, Indonesia, Turkey, and Spain. More attacks are in the planning stages, and U.S. lives and property are being actively targeted by al-Qa'ida and other terrorist organizations that have death and destruction as their principal goals.

We learned some painful lessons on September 11, 2001. We learned that while we had developed a wide array of U.S. Government counterterrorism capabilities and accrued a vast amount of information about those who would do us harm, we lacked a government-wide ability to integrate knowledge, data systems, expertise, mission, and capabilities, which are the critical weapons in the fight against terrorism. It is only through such integration of effort that we will be able to prevent future 9/11s.

As we strive as a nation to create such a framework, a key objective of the U.S. Government's counterterrorism strategy today is to ensure that all agencies and departments involved in the fight against terrorism share threat information and finished analysis that can be used to prevent terrorist attacks. At the direction of the President, TTIC began its mission May 1, 2003, specifically to achieve this objective for counterterrorism analysis.

TTIC represents a new way of optimizing the U.S. Government's knowledge and formidable capabilities in the fight against terrorism. For the first time in our history, a multi-agency entity has

access to information systems and databases spanning the intelligence, law enforcement, homeland security, diplomatic, and military communities that contain information related to the threat of international terrorism. In fact, TTIC has direct-access connectivity with 14 separate U.S. Government networks -- with connectivity to another 10 networks planned -- enabling information sharing as never before in the U.S. Government. This unprecedented access to information allows us to gain a comprehensive understanding of terrorist threats to U.S. interests at home and abroad and, most importantly, to provide this information and related analysis to those responsible for detecting, disrupting, deterring, and defending against terrorist attacks.

A key objective of TTIC is to develop an integrated information technology architecture so that sophisticated analytic tools and federated search capabilities can be applied to the many terabytes of data available to the Federal Government. We must be able to cross check these different data sets, which are collected by departments and agencies statutorily authorized to do so, in a manner that allows us to identify terrorists and their supporters before they reach our shores or when they emerge within our midst. Simply put, we need to create new knowledge from existing information. We can do this, with complete respect for the privacy rights of U.S. persons and in accordance with the Constitution, as we work together in a collaborative and integrated manner.

There exists within the TTIC "joint venture" real-time collaboration among analysts from a broad array of agencies and departments who sit side-by-side, sharing information and connecting the scattered pieces of the terrorism puzzle. These partners include not only the FBI, CIA, and the Departments of State, Defense, and Homeland Security, but also other Federal agencies and departments, currently including the Capitol Police, the Department of Energy, and the Nuclear Regulatory Commission. Other federal departments and agencies have been invited to join.

- As envisioned by the President, this physical integration of expertise and sharing of information enables and empowers the key organizations involved in the fight against terrorism. Collectively, they are fulfilling their shared responsibilities in a fused environment, "doing business" jointly as TTIC. This fusion and synergy will be further enhanced when TTIC and most of CIA's Counterterrorist Center and FBI's Counterterrorism Division collocate at a state-of-the-art facility this summer.

- This integrated business model not only capitalizes on our respective and cumulative expertise, but it also optimizes analytic resources in a manner that allows us to cover more effectively and comprehensively the vast expanse of terrorist threats that will face the Homeland and U.S. interests worldwide for the foreseeable future.

- In simple terms, we are closing the seams among U.S. Government entities engaged in the identification and analysis of terrorism information.

The integration of perspectives from multiple agencies and departments represented in TTIC is serving as a force multiplier in the fight against terrorism. On a strategic level, TTIC provides the President and key Cabinet officials a daily analytic product on the most serious terrorist threats and related terrorism information that serves as a common foundation for decision-making regarding the actions necessary to disrupt terrorist plans. Rather than multiple threat assessments and disparate information flows on the same subject matter being forwarded separately to senior policymakers, information and finished analysis are now fused in a multi-agency environment so that an integrated

and comprehensive threat picture is provided. If there are analytic differences on the nature or seriousness of a particular threat, they are incorporated into the analysis.

Similar mechanisms transform threat information and analysis into alerts and advisories in order to better prepare the Nation as well as to warn targets of potential terrorist attacks.

- For example, TTIC issued a terrorist threat alert at 11:00 p.m. on 20 December of last year, which triggered senior-level discussions and a subsequent decision before noon the following day to raise the national threat condition level to "orange."

- TTIC's analytic assessments also have had an impact overseas. TTIC advisories, warnings, and alerts about threats to U.S. interests in the Middle East, Europe, and Southeast Asia have prompted reviews and adjustments of security postures and procedures at various locations over the past year.

- As part of this warning and analytic orchestration role, TTIC has been designated by the Director of Central Intelligence to lead an integrated Intelligence Community analytic effort focusing on the potential terrorist threat to the 2004 Summer Olympics in Greece.

In addition to connecting the proverbial intelligence "dots" and doing analytic assessments, TTIC also is actively working to ensure that terrorist threat information and finished analysis are disseminated to those who play a role in protecting U.S. interests at home and abroad. For example, TTIC sponsors a top secret website, TTIC Online, that has in excess of 3 ½ million terrorism-related documents at various levels of classification from the intelligence, law enforcement, homeland security, diplomatic, and military communities.

- TTIC Online currently is available to over 2,600 users at every major Federal department and agency involved in counterterrorism activities.

- In the coming months, TTIC Online will be replicated at lower classification levels that will enhance the ability of DHS and FBI to make more terrorism-related material available to state and local government officials, law enforcement entities, and the private sector.

In addition, a joint information-sharing program office of TTIC partner agencies is currently focused on addressing key impediments to the free flow of terrorism-related information.

- The Intelligence Community traditionally has used a marking called "ORCON," or "Originator Control," which limits the dissemination of intelligence reports. The Intelligence Community has reduced the percentage of terrorism-related ORCON documents by about half since the latter part of 2001, from approximately 11 percent then to 6 percent now.

- In addition, significant progress has been made by the Intelligence Community on the use of "tear-line" reporting -- reporting where sensitive sources and methods information has been removed so the information can be disseminated in a timely manner to a broader audience. The availability and use of tear-lines has increased nearly 70 percent since 2001.

Under Homeland Security Presidential Directive 6 of September 2003, TTIC is also responsible for integrating and maintaining a single repository of all U.S. Government international terrorist identities information in support of a streamlined Government-wide system for "watchlisting" and terrorist screening activities. To date, TTIC has approximately 100,000 known or suspected international terrorist identities catalogued. This information is provided to the FBI-administered Terrorist Screening Center, which ensures that front line law enforcement officers, consular officials, and immigration and border personnel have the capability to rapidly screen individuals known or suspected to be terrorists before they enter the United States.

I cannot tell you that all of these efforts have enjoyed smooth sailing, as there are many challenges associated with what is, in essence, the crafting of a new national terrorism analysis and information-sharing framework to better protect this nation. We need to implement this revolutionary concept in a thoughtful and evolutionary fashion, as my colleagues on this panel are actively engaged in fighting a global war against terrorism, and I believe that we cannot afford to adversely affect these activities by dislocations associated with organizational change or abrupt shifts in analytic responsibility. In particular, this new national framework for the cross-government integration of information systems, expertise, and analytic missions should not come at the expense of operational, collection, covert action, and investigative activities of our Intelligence, Law Enforcement, and Homeland Security Communities.

As we continue in what is destined to be a multiyear battle against the deadly forces of international terrorism, my colleagues and I have a special obligation to learn from the painful lessons of 9/11 and to continue the task of implementing a national counterterrorism system and strategy that maximizes the security and safety of all Americans, wherever they live or work. In my personal opinion, the organizational and information-sharing status quo that existed on September 11, 2001 was inadequate to safeguard America. While significant progress has been made since then, I believe that we, as a government and as a nation, are not yet optimally configured to deal with the terrorist threat. This Commission, with its studied and comprehensive review of the events and factors that resulted in the tragedies in New York, the Pentagon, and the fields of Pennsylvania, is ideally suited to take a fresh look at how all the eclectic parts of the national counterterrorism effort fit together and whether we need to adopt new and better ways to organize ourselves. It is only by enhancing the security of Americans everywhere that we will truly honor the lives and the sacrifice of those who died more than two-and-a-half years ago.