Testimony of

Mr. Vance Hitch

April 17, 2002

Mr. Chairman and Members of the Committee, I am pleased to appear before you today to discuss information sharing. I am both honored and grateful for this opportunity.

Last month, the Attorney General appointed me Chief Information Officer (CIO) for the Department of Justice. In announcing my appointment, the Attorney General stated: "A critical element in our battle against the terrorist threat is the effective use of information technology to share information across law enforcement." To pursue this mission, my mandate is clear: upgrade the Department's information technology program to better enable core mission accomplishment, and use information technology as a tool for collaboration among Justice components, between Justice and other federal agencies, and among federal, state, and local law enforcement.

In the aftermath of the September 11 terrorist attacks, it is clear that information sharing is critical to our nation's safety. The Attorney General recognizes clearly that access to accurate and timely information is crucial to supporting the Department's critical law enforcement responsibilities, and especially in protecting against acts and threats of terrorism. Improving and expanding the Department's use of information technology are key components of the Attorney General's wartime reorganization of the Department, announced on November 8, 2001.

Just last week, the Attorney General directed key Justice components to take further actions to institutionalize the Department's ongoing efforts to coordinate information relating to terrorism. Specifically, he ordered the investigating components to establish procedures to provide, on a regular basis and in electronic format, the names, photographs and other identifying data of all known or suspected terrorists for inclusion in the State Department's TIPOFF system, the FBI's National Crime Information Center (NCIC), and the Customs Service's Interagency Border Inspection System (IBIS). He also ordered the Assistant Attorney General for Legal Policy to work with the components to draft for his consideration procedures, guidelines, and regulations to implement the information sharing provisions of the USA PATRIOT Act.

Historically, information systems have been developed and implemented to meet the particular business needs of a specific component organization. The result, as you know all too well, is a number of legacy stovepipe systems that impede cross component information sharing. However, even before 9/11, the Department was involved in several efforts to improve sharing or to consolidate systems. For example:

· El Paso Intelligence Center (EPIC). The Department of Justice established the El Paso Intelligence Center (EPIC) in 1974, staffed by representatives of the INS, the Customs Service, and the DEA, to provide a common information resource on drug movement and immigration violations. Today, EPIC has grown to include 15 federal agencies, the Texas Department of

Public Safety, and the Texas Air National Guard. In addition, EPIC maintains information sharing agreements with other federal law enforcement agencies, the Royal Canadian Mounted Police and each of the 50 states and serves law enforcement agencies throughout the western hemisphere. A telephone call, fax, or teletype from any of these agencies provides the requestor real-time information accessed through EPIC from many different federal databases, plus EPIC's own internal database.

· IDENT/IAFIS. The IDENT/IAFIS project was established to integrate the INS IDENT system with the FBI's IAFIS. The integration project will directly enhance the Department's ability to meet its mission through increased apprehension and effective prosecution of criminal aliens. It is a major cross-cutting initiative and will provide improved INS identification services to determine whether a person they apprehend is the subject of a posted Want or Warrant or has a record in the FBI's Criminal Master File. Similarly, it will provide law enforcement agencies with all relevant immigration information as part of a criminal history response from a single FBI.

· Joint Automated Booking System (JABS). JABS is another major cross-cutting initiative involving the Bureau of Prisons, the U.S. Marshals Service, the INS, the FBI, and the DEA. JABS streamlines the identification and processing of federal offenders by providing the means to electronically collect, store, and transmit photographic, fingerprint, and biographical data.

More recently, and in direct response to the deadly attacks on the World Trade Center and the Pentagon, the President directed the Department to create a Foreign Terrorist Tracking Task Force (FTTTF). This is a multi-agency Task Force that combines agency expertise, information and advanced technologies to identify, locate, and remove or deny entry to foreign terrorists and their supporters. There are several federal agencies that are already participating (e.g., the FBI, the INS, the State Department, the Customs Service, the Social Security Administration, and elements of the Intelligence Community). These agencies are joint participants with a common mission of neutralizing the threat of terrorist aliens.

The President also directed that the Attorney General and the Director of Central Intelligence "ensure, to the maximum extent permitted by law, that the Task Force has access to all available information necessary to perform its mission." The Task Force is both gathering and analyzing data contributed by participating agencies, using advanced methods to mine the data, establish patterns, and calculate risk parameters. Results of these analyses are provided to the relevant agencies for appropriate enforcement action. Although the Task Force is still in the early stages of its work, it offers an especially promising model for information sharing and collaboration.

Despite these efforts, it is clear that more needs to be done. To meet the new threats and challenges we face today, we must fundamentally rethink how information systems are designed, developed and managed so that IT fosters, rather than hinders, collaboration. This means creating a DOJ information architecture, infrastructure, and management approach that promote both information sharing and information security.

It is important that we move forward on both the sharing and security fronts simultaneously. Sharing information depends in no small measure on our ability to assure that the information

will be protected from unauthorized disclosure. A primary obstacle to sharing has been, and remains, concerns about the security of the information once it is outside the control of the agency that "owns" it.

The Department has a long ways to go, but I am confident we are headed in right direction. I am convinced that organizational and cultural roadblocks to information sharing are being remedied. In part, this is because of Executive Branch and Congressional leadership; in part, it is because of the sheer magnitude and complexity of the threat. We know that to succeed we must work together. Our long-term goal -- and one that technology can help make a reality -- is that the Department of Justice and all members of the law enforcement community, whether federal, state, or local, be able to communicate and collaborate with one another fully, easily, and securely.

One of the Attorney General's top ten management goals, and one of his initial assignments to me, is the development of a comprehensive Information Technology Plan for the Department. We are working on this Plan and expect to complete it within the next month. However, let me briefly outline the Plan's major themes and directions:

* Information Sharing
There are three key technical barriers to information sharing within the Department of Justice: (1) insufficiently modernized office automation systems; (2) inadequate networking; and (3) applications and data stores that cannot be accessed by other components or agencies. Overcoming these barriers is a long-term effort, but progress has and is being made. For example, the components are in various stages of updating their office automation and networking infrastructures and, as mentioned earlier, there have been some, albeit limited, efforts to share information and integrate systems.

Critical areas in support of information sharing to be addressed in the plan include:
o Upgrading our telecommunications infrastructure to improve cross component access to intranet sites and other data stores, meet projected demands for bandwidth, and ensure wireless and remote access to the DOJ network;
o Accelerating the completion of component office automation upgrades; and
o Modernizing access methods, such as through Web-like interfaces, collaboration platforms, and systems consolidation.

I want to elaborate on the last point. Of great concern to this Committee is whether agencies are sharing information related to foreign nationals who want to enter this country, or are already here, and who may be threats to national security. One of the difficulties is that the INS has an array of heterogeneous systems that does not provide a full and complete picture of a foreign national's travel to and from the United States or critical events during his or her period of stay. For this reason, the Department is exploring with the Office of Homeland Security and affected agencies the creation of a consolidated database that would be organized by person rather than immigration event and would be accessible to all parties, including the State Department and the Customs Service.

Information Security
Information systems must be protected from inadvertent or deliberate disclosure of sensitive

information to unauthorized users, from attacks on the infrastructure that deny services, and from attempts to alter or otherwise falsify information. Securing our information systems has rightfully become the focus of increasing scrutiny by the Congress and others.

We need to improve information security by building a long-term Department-wide security infrastructure that will ensure that information systems are secure from day one, rather than requiring continuous patches and fixes. In the meantime, we will take two immediate steps:

o First, we need to make sure that existing systems are as well protected as they should be by identifying vulnerabilities and taking corrective action. The Department is carefully monitoring and tracking component progress in this regard.

o Second, we need to build infrastructure-based capabilities, such as public key infrastructure, available for use throughout DOJ and scalable to the broader law enforcement and judicial communities.

IT Planning and Management

We also intend to strengthen the way we plan for and manage our IT investments. Here again, progress has been made but more work is needed. Among my priorities will be developing an enterprise architecture that is linked to investment management and provides a foundation for ensuring that IT systems meet mission requirements, identifies redundancies and opportunities for consolidation, and ensures cross component sharing of common assets, services, and solutions. It will be an architecture that ensures secure access to data by all authorized users and promotes sharing and collaboration across organizational lines. Relatedly, I will be emphasizing the development of Department-wide standards and policies, as well as stronger oversight of priority initiatives.

This is an ambitious agenda, one that will take time, resources, and cooperation to implement fully. But I can assure this Committee that the Department of Justice is committed to moving away from stovepipe information systems, overcoming unnecessary obstacles to information sharing, and working closely with the Office of Homeland Security, federal agencies, and others to fully and securely share sensitive law enforcement. We simply cannot afford to do otherwise.

Again, thank you for the opportunity to discuss this matter of critical importance to the Justice Department, and to all law enforcement. I would be pleased to respond to your questions at this time.