Testimony of

Mr. Michael Cronin

October 9, 2002

GOOD MORNING MADAM CHAIRWOMAN, AND MEMBERS OF THE SUBCOMMITTEE. I appreciate the opportunity to participate in this hearing concerning coordinated information sharing among Federal agencies in the war against terrorism. Since September 11, we at the Immigration and Naturalization Service (INS) have seen an unprecedented sharing of data and knowledge among federal agencies.

Congress signaled its support for these efforts by enacting the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act (P.L. 107-56) which became law on October 26, 2001, and the Enhanced Border Security and Visa Entry Reform Act of 2002 (P.L. 107-173) which became law on May 14, 2002. As you know, this legislation requires the INS to fully integrate all of its databases and data systems that process or contain information on aliens. This integrated systemintegration will become part of the interoperable electronic data system, called Chimera. This system, Wwhen completed, Chimera will provide current and immediate access to information in law enforcement and intelligence databases relevant to determine whether to issue a visa and to determine the admissibility of an alien.

The INS is one of the core agencies that require enhanced information sharing capabilities. We need to tap into additional external sources of data to support our enforcement and intelligence functions, and we recognize that the data we collect can be crucial to the law enforcement and intelligence communities to combat the threat of terrorism. Efforts to improve the quality and timeliness of information access will strengthen our ability to prevail against the threat of terrorism while limiting the disruption to legitimate commerce that might otherwise arise.

Madam Chairwoman let me begin by describing some important things we are already accomplishing to meet these challenges. As you know, the Office of Homeland Security, in conjunction with the Office of Management and Budget, is overseeing initiatives that promote information sharing between Federal agencies horizontally, and then from those agencies to State and local governments. We also are working internationally to develop better ways of sharing information that will support international enforcement and intelligence operations.

I cannot over-emphasize the commitment of the INS and other participants to work together in order to achieve a more supportive and comprehensive information environment.

Prior to September 11, the INS shared data in many ways with other agencies in support of law enforcement efforts. Since then we have redoubled our efforts to contribute data and information that have supported counter-terrorism intelligence, investigative, and enforcement operations.

For many years, the INS has taken steps to enhance the exchange of information through greater cooperation among the law enforcement community. As early as 1985, the INS was sharing vital information with the U.S. Customs Service through the Interagency Border Inspection System (IBIS), the primary automated screening tool currently used by Customs and the INS to which many Federal agencies contribute lookout information. Since that time, we have put in place a number of other initiatives to exchange information with other entities, which are in various stages of implementation.

For example, in October 2001, INS Commissioner James Ziglar and Assistant Secretary of State for Consular Affairs Mary Ryan jointly agreed to begin transmitting data from the Department of State's Consolidated Consular Database to IBIS that includes nonimmigrant visa issuance information and a photograph of the alien. Because of that cooperation, the alien's photograph is now available at our ports-of-entry to determine if the alien engaged in any document fraudulent conduct. That deployment was completed in January 2002. In Miami, where access to the data was first instituted, INS Inspectors credit the initiative with detecting 108 fraudulent visa holders in the first six months. INS Inspectors using this data in New York caught an alien trying to enter the US on a falsified Russian diplomatic passport. In another instance, a 41-year old man was discovered using the altered visa of a three-year old Brazilian boy.

Another example involves the sharing of fingerprint data. Prior to September 11, the INS had worked with the U.S. Marshals Service to incorporate fingerprint data of their wanted persons into the INS fingerprint identification system known as IDENT. After September 11, the INS worked with the Federal Bureau of Investigation (FBI) to incorporate fingerprint data from their Integrated Automated Fingerprint Information System (IAFIS) "wants and warrants" file into IDENT as well. IAFIS contains fingerprints for persons wanted by Federal, State, and local law enforcement agencies. This effort has been extremely successful and has already resulted in the identification and apprehension of over 3,100 individuals wanted for felony crimes.

The Federal Government maintains a number of databases that provide real-time information to foreign diplomatic outposts, border ports-of-entry, and interior domestic law enforcement. We work closely with other federal agencies to maintain these databases to prevent terrorists from entering the United States, to detect and apprehend those already in the country, and to gather intelligence on terrorist plans and activities or conspiracies.

Examples of systems that share data include:

? The Department of State TIPOFF System--designed to alert [WHO?] of suspected terrorists who are not U.S. citizens as they apply for visas overseas or as they attempt to pass through U.S., Canadian, and Australian border entry points.

? The FBI's National Crime Information Center--the nation's principal law enforcement automated information sharing tool. It provides on-the-street access to criminal history information to over 650,000 Federal, State, and local law enforcement officers.

? The Interagency Border Inspection System (IBIS)--the primary automated screening tool used by both the INS and U.S. Customs Service at ports-of-entry. The inclusion of data on terrorists in this integrated database helps preclude the entry of known and suspected terrorists into the U.S., warn inspectors of a potential security threat, and alert intelligence and law enforcement agencies that a suspected terrorist is attempting to enter the U.S. at a specific location and time.

Let me now discuss other key programs that INS is undertaking related to the USA PATRIOT Act and the Enhanced Border Security and Visa Entry Reform Act of 2002. Under the conceptual framework of creating a U.S. entry-exit system, INS and the Department of Justice have implemented the National Security Entry Exit Registration System (NSEERS). Also related to this effort are the expanded use of electronic passenger manifests, the Student and Exchange Visitor Information System (SEVIS), and the continuing development of the use of biometrics in travel documents.

Development of an Entry Exit System

An integrated entry-exit control program that records and matches the arrival and departure of non-U.S. citizens enhances the security of the United States by providing government officials with specific information about who is entering the country and who is staying past their period of authorized admission. Managing the entry, stay and departure of alien visitors is a major component of controlling our borders and requires collecting information regarding the movement of aliens in, through, and out of the United States. Armed with this information, the United States Government can make better-informed policy and management decisions, identify and take action against those who violate the law, more easily locate individual aliens of interest to law enforcement entities, and validate the immigration status of aliens so that only eligible persons receive immigration benefits. At the same time, we remain mindful that any process required to support an Entry Exit program must facilitate legitimate travel and commerce so we do not adversely affect the economies of the United States and its neighbors.

In order to effect the creation of an integrated entry exit system in a timely manner, the INS established an interagency project team. Consisting of members from the Departments of Justice, State, Treasury, and Transportation - those agencies with principal responsibility for managing the U.S. borders - the project team defines their mission in terms of "managing the people, cargo, and means of conveyance crossing U.S borders." The U.S. Entry Exit Program is a joint effort by these Departments whose intent is to significantly improve the processes, policies, workforce, and systems utilized to manage the pre-entry, entry, stay, and exit of international travelers through over 300 ports-of-entry.

The Entry Exit Program will also facilitate collaboration across the Border Management Community through tighter integration of processes and data relevant to travelers, cargo, and means of conveyance. And lastly, the Program will foster greater cooperation with Federal, State, and local intelligence and law enforcement organizations through improved access to more complete and timely data generated by the Border Management Community, as well as information generated by State and local law enforcement where the assistance of the Federal law enforcement community is requested.

Electronic Passenger Manifests

INS has already taken the first steps in developing the entry exit system. Since January 2002, air carriers have been required to submit passenger and crew arrival information electronically to the US Customs Service. INS is able to acess this information via IBIS. The electronic transmission of manifests is a critical piece of the Entry Exit System. The Advance Passenger Information System (APIS) [Creates consistency with Page 9 reference to APIS] allows the INS to conduct analysis and identify and apprehend national security threats as well as criminals. With the addition of electronic departure data, the INS will be able to improve not only our ability to identify and apprehend National Security Threats and criminals but also improve our ability to provide valid overstay data.

On October 1, 2002, the INS began accepting passenger data electronically for both arriving and departing passengers who arrived in the United States by air or sea carrier under the visa waiver program. This new initiative implements the requirements that had been set forth in the Visa Waiver Permanent Program Act of 2000. The next step involving electronic manifest will occur on January 1, 2003, when air and sea carriers will be required to transmit electronic arrival and departure data for all arriving and departing passengers including new data elements which will

aid in the identification of mala fide travelers.
The information captured from the electronic manifests feeds into the Arrival Departure Information System (ADIS). The ADIS will be the repository for arrival and departure records for non-citizens. The ADIS will match arrival and departure records to accurately identify those individuals who are out of status. In order to do this, the system will need to interface with several systems inside and out of INS. The system will also need to interface with Department of State systems to update visa records to show when individuals overstay their authorized stay. The Immigrant Services Division (ISD) case management systems will need to interface with ADIS to pass any adjustment of status or extension of stay information.

National Security Entry Exit Registration System (NSEERS)

We have also taken the initiative to expand our knowledge through the National Security Entry-Exit Registration System (NSEERS). The INS began to implement at NSEERS at U.S. ports-of-entry on September 11, 2002. Under NSEERS, INS is fingerprinting in IDENT and photographing certain nonimmigrant aliens who may potentially pose a national security risk upon their arrival in the United States. In addition, these non-immigrant aliens are required to register periodically with the INS, allowing us to better verify that they are complying with the terms of their nonimmigrant status.
Nonimmigrant aliens subject to special registration provide specific information and have their fingerprints and photograph taken upon their arrival into the United States (US). They must update their registration information approximately 30 days after arrival, every twelve months after arrival, and upon certain events (such as changes of address, employment, or school). Finally they must record their departure from the United States from designated locations. Approximately 100,000 people per year will be registered through this program.
Use of Biometrics

Another important piece of the system involves the use of biometrics. Currently the National Institute of Standards and Technology (NIST) is working expeditiously to identify and define biometric standards. These tests are being conducted so that the NIST can provide guidance to the Attorney General and Secretary of State, who are responsible for setting standards to be used in United States issued travel documents. All United States travel documents issued to aliens must include biometric identifiers if the documents are issued on or after October 26, 2004. Since 1998, the DOS and INS have produced over five million Border Crossing Cards that include biometrics. The Border Crossing Card has two fingerprints and a digital photograph imbedded in an optical stripe. The INS will shortly begin testing biometric verification systems at six Portsports-of-Entryentry. The Space and Naval Warfare System Center, San Diego (SPAWAR) has been contracted to conduct this evaluation. The INS has awarded two contracts for Optical Reader/Writer and Biometrics Verification Systems that will be used for this test. The SPAWAR will conduct tests, gather the metrics, and evaluate the concept of BCC Biometric Verification Systems (BVS) at different inspection ports-of-entry and climatic environments. The test will consist of 30 optical stripe (laser card) readers and biometric verification systems at small, medium and large land and air ports-of-entry. The designated ports are Los Angeles, San Ysidro, Nogales, Falcon Dam, San Antonio, and Atlanta. The testing process will help ensure that whatever biometric equipment is ultimately put in place will meet the needs of the entry exit

system. If the evaluation is successful the INS will begin the procurement process to deploy these biometric verification systems along the border.

Student and Exchange Visitor Information System (SEVIS)

The INS has made considerable progress in implementing a new system that will greatly enhance our ability to track and monitor foreign students and exchange program visitors. This progress leaves us confident that we will meet the January 1, 2003 deadline for full implementation as established in the USA PATRIOT Act. This Internet-based system, known as the Student and Exchange Visitor Information System (SEVIS), will maintain critical, up-to-date information about foreign students and exchange visitors, and their dependents, and will allow for electronic access to this information. As such, it will enable the INS to track students in the United States more accurately and more expeditiously. SEVIS, as a fully implemented system, will be an integrated system that incorporates information directly from schools, exchange programs, several INS systems, and the DOS.

The INS deployed the core operational component of SEVIS and began accepting and reviewing school petitions for eligibility (Form I-17) as of July 1. As of October 7, 2002, there were 2,625 schools currently in various stages in the system, with 1,090 approved schools issuing and updating student records electronically in SEVIS. Also as of October 7, 692 schools had completed and submitted an electronic petition and were awaiting approval to use SEVIS. Another 870 schools created and saved drafts of such petitions but had not yet submitted a completed petition for adjudication. Upon approval, these schools will be able to access SEVIS to create and update student records.

To help facilitate effective implementation of SEVIS, the INS has worked closely with many education associations including the American Council on Education, the Association of International Educators, the National Association of State Universities and Land-Grant Colleges, and the California Community Colleges Chancellor's Office. Further, INS has established a SEVIS-dedicated, national call center with multiple tiers to answer technical and policy-related questions.

The INS is exerting greater control over the institutions authorized to admit foreign students in F and M visa status. The INS believes that for this brand new SEVIS system, review of all schools is the best method to ensure integrity. To facilitate the review of INS-approved schools and to ensure the enrollment of eligible schools in SEVIS in a timely manner, the INS has implemented a two-phased process for school review and SEVIS enrollment. Phase 1 was a preliminary enrollment period in which schools that have been INS-approved for at least the last three years to admit foreign students and are recognized as accredited or Title IV by the Department of Education were reviewed and granted access to SEVIS. Phase 2 will involve the certification of a school after a full review, including an on-site visit in many cases. For some schools, the on-site visit will verify their bona fides, but more importantly, the on-site visit will help ensure record keeping and reporting compliance, as well as confirm that the schools are aware of their responsibilities. An interim rule that will explain the school certification process has been published.

The INS is working toward enhancing our data share arrangement with the DOS Office of Consular Affairs in order to electronically provide SEVIS data for verification during the visa

issuance process. INS and DOS currently have a Nonimmigrant Visa (NIV) Datashare arrangement, whereby DOS is sending all nonimmigrant visa issuance data to INS and Customs systems. SEVIS plans to extract data of all the F (academic), M (vocational), and J (exchange visitor) records from that existing arrangement.

The SEVIS program staff have been working closely with the INS Entry/Exit program staff in order to collect data, such as date and port-of-entry as mandated by the USA PATRIOT Act. SEVIS has been included in the functional requirements for phase 1 of a comprehensive entry/exit system. Phase 1 consists of the Visa Waiver Permanent Program Act (VWPPA) Support System, which leverages existing information technology systems, specifically the Advance Passenger Information System (APIS) and the Arrival Departure Information System (ADIS) to capture data electronically. This first phase of the entry/exit system will provide entry data on all F, M and J aliens to SEVIS at all air and sea Ports-of-Entry. For those Ports-of-Entry not yet included in the entry/exit system, we will have alternative processes to provide data to SEVIS and notice to the schools.

The Enhanced Border Security and Visa Entry Reform Act (Border Security Act) of 2002 requires schools to report the failure of a foreign student to enroll within 30 days after the schools' registration deadline. The INS has established a toll-free, 1-800, number for schools to report a foreign student's failure to enroll, and once all schools are enrolled they will be able to report directly in SEVIS. The INS is also required by this legislation to review all schools every two years to ensure compliance with record-keeping and reporting requirements.

Full implementation of SEVIS will revise and enhance the process by which foreign students and exchange visitors gain admission to the United States. The INS, through SEVIS, will increase its ability to track and monitor foreign students and exchange visitors in order to ensure that they arrive in the United States, show up and register at the school or exchange visitor program, and properly maintain their status during their stay as valued guests in this country.

Conclusion

Madam Chairwoman, having addressed what we have been doing to deal with the immediate challenges in response to guidance from Congress and the Administration, let me turn to the activities that address emergent issues on the horizon.

To improve in the information technology area, the management principle to develop information systems is to build on a sound strategic foundation. The INS has established important mechanisms to address these principles internally. One of these mechanisms is our formal Enterprise Architecture and technical architectures. In May 2000, the INS initiated a project to develop a business-driven Enterprise Architecture (EA). The result of the project is a multi-year IT modernization plan whose implementation will require consistent oversight, funding, and systems development. The EA Plan was completed on schedule and on budget in July 2002. The EA Plan provides the blueprint and build-out plan for modernizing information systems and technical infrastructure that will enable the INS to better meet its business objectives. In addition, an Information Technology Investment Management (ITIM) process has been in place for over three years. ITIM is the standardized process by which investment dollars are approved for information technology (IT) projects. This process ensures that IT investments are spent wisely and coordinated among INS components. In doing so, we are mindful of the relationships that we must support with our technical enhancements while integrating our business objectives and developing technical solutions.

Thank you Madam Chairwoman for this opportunity to share my views with you and the Committee. I will be happy to answer any questions you may have at this time.

# # #