AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

FEDERAL INTERAGENCY DATA-SHARING AND NATIONAL SECURITY

HEARING

BEFORE THE

SUBCOMMITTEE ON NATIONAL SECURITY, VETERANS AFFAIRS AND INTERNATIONAL RELATIONS

OF THE

COMMITTEE ON GOVERNMENT REFORM

HOUSE OF REPRESENTATIVES

ONE HUNDRED SEVENTH CONGRESS

FIRST SESSION

JULY 24, 2001

Serial No. 107–100

Printed for the use of the Committee on Government Reform

Available via the World Wide Web: http://www.gpo.gov/congress/house
http://www.house.gov/reform

U.S. GOVERNMENT PRINTING OFFICE

81–594 PDF WASHINGTON : 2002

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

COMMITTEE ON GOVERNMENT REFORM

DAN BURTON, Indiana, *Chairman*

BENJAMIN A. GILMAN, New York
CONSTANCE A. MORELLA, Maryland
CHRISTOPHER SHAYS, Connecticut
ILEANA ROS-LEHTINEN, Florida
JOHN M. MCHUGH, New York
STEPHEN HORN, California
JOHN L. MICA, Florida
THOMAS M. DAVIS, Virginia
MARK E. SOUDER, Indiana
JOE SCARBOROUGH, Florida
STEVEN C. LATOURETTE, Ohio
BOB BARR, Georgia
DAN MILLER, Florida
DOUG OSE, California
RON LEWIS, Kentucky
JO ANN DAVIS, Virginia
TODD RUSSELL PLATTS, Pennsylvania
DAVE WELDON, Florida
CHRIS CANNON, Utah
ADAM H. PUTNAM, Florida
C.L. "BUTCH" OTTER, Idaho
EDWARD L. SCHROCK, Virginia
JOHN J. DUNCAN, JR., Tennessee

HENRY A. WAXMAN, California
TOM LANTOS, California
MAJOR R. OWENS, New York
EDOLPHUS TOWNS, New York
PAUL E. KANJORSKI, Pennsylvania
PATSY T. MINK, Hawaii
CAROLYN B. MALONEY, New York
ELEANOR HOLMES NORTON, Washington, DC
ELIJAH E. CUMMINGS, Maryland
DENNIS J. KUCINICH, Ohio
ROD R. BLAGOJEVICH, Illinois
DANNY K. DAVIS, Illinois
JOHN F. TIERNEY, Massachusetts
JIM TURNER, Texas
THOMAS H. ALLEN, Maine
JANICE D. SCHAKOWSKY, Illinois
WM. LACY CLAY, Missouri
DIANE E. WATSON, California
——— ———
———
BERNARD SANDERS, Vermont (Independent)

KEVIN BINGER, *Staff Director*
DANIEL R. MOLL, *Deputy Staff Director*
JAMES C. WILSON, *Chief Counsel*
ROBERT A. BRIGGS, *Chief Clerk*
PHIL SCHILIRO, *Minority Staff Director*

SUBCOMMITTEE ON NATIONAL SECURITY, VETERANS AFFAIRS AND INTERNATIONAL RELATIONS

CHRISTOPHER SHAYS, Connecticut, *Chairman*

ADAM H. PUTNAM, Florida
BENJAMIN A. GILMAN, New York
ILEANA ROS-LEHTINEN, Florida
JOHN M. MCHUGH, New York
STEVEN C. LATOURETTE, Ohio
RON LEWIS, Kentucky
TODD RUSSELL PLATTS, Pennsylvania
DAVE WELDON, Florida
C.L. "BUTCH" OTTER, Idaho
EDWARD L. SCHROCK, Virginia

DENNIS J. KUCINICH, Ohio
BERNARD SANDERS, Vermont
THOMAS H. ALLEN, Maine
TOM LANTOS, California
JOHN F. TIERNEY, Massachusetts
JANICE D. SCHAKOWSKY, Illinois
WM. LACY CLAY, Missouri
——— ———
——— ———

EX OFFICIO

DAN BURTON, Indiana
HENRY A. WAXMAN, California

LAWRENCE J. HALLORAN, *Staff Director and Counsel*
THOMAS COSTA, *Professional Staff Member*
JASON CHUNG, *Clerk*
DAVID RAPALLO, *Minority Counsel*

CONTENTS

	Page
Hearing held on July 24, 2001	1
Statement of:	
Swartz, Bruce C., Deputy Assistant Attorney General, Criminal Division, U.S. Department of Justice; Bruce Townsend, Special Agent in Charge, Financial Crimes Division, U.S. Secret Service; Catherine Barry, Director, Consular Affairs Visa Services, accompanied by John Brennan, Visa Office, Interagency and Systems Liaison Division, U.S. Department of State; and Colonel Mike Deacy, USAF, Assistant Deputy Director, Information Engineering, Defense Information Systems Agency	5
Letters, statements, etc., submitted for the record by:	
Barry, Catherine, Director, Consular Affairs Visa Services, prepared statement of	30
Deacy, Colonel Mike, USAF, Assistant Deputy Director, Information Engineering, Defense Information Systems Agency, prepared statement of	46
Shays, Hon. Christopher, a Representative in Congress from the State of Connecticut, prepared statement of	3
Swartz, Bruce C., Deputy Assistant Attorney General, Criminal Division, U.S. Department of Justice, prepared statement of	9
Townsend, Bruce, Special Agent in Charge, Financial Crimes Division, U.S. Secret Service, prepared statement of	22

FEDERAL INTERAGENCY DATA-SHARING AND NATIONAL SECURITY

TUESDAY, JULY 24, 2001

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON NATIONAL SECURITY, VETERANS AFFAIRS AND INTERNATIONAL RELATIONS,
COMMITTEE ON GOVERNMENT REFORM,
Washington, DC.

The subcommittee met, pursuant to notice, at 10 a.m., in room 2247, Rayburn House Office Building, Hon. Christopher Shays (chairman of the subcommittee) presiding.

Present: Representatives Shays, Gilman, Otter, and Kucinich.

Staff present: Lawrence J. Halloran, staff director and counsel; Robert Newman and Thomas Costa, professional staff members; Alex Moore, fellow; Jason M. Chung, clerk; Kristin Taylor, intern; David Rapallo, minority counsel; Earley Green, minority assistant clerk; and Teresa Coufal, minority staff assistant.

Mr. SHAYS. Good morning.

In 1996, President Clinton declared international crime a threat to national security and ordered Federal agencies to integrate and coordinate their efforts against global crime syndicates. In response, the Department of Justice [DOJ], launched the Anti-Drug Network/Nigerian Crime Initiative, referred to as ADNET/NCI, the first data-sharing project allowing all participating Federal law enforcement agencies to pool active criminal case information on a secure network, computer network.

It was hoped this initiative would help meet the threats of money laundering, narcotics trafficking and terrorism, and serve as a prototype for more efficient data base coordination and cooperation. But now it appears that the ADNET/NCI project has lost momentum, falling prey to jurisdictional disputes, unresolved legal issues, bureaucratic inertia, budget constraints and personnel turnover. A key leadership position in the program has been vacant for months. What were once regular working group meetings have become sporadic. A number of ADNET/NCI task force sites appear to lack agency support.

During our hearing last April on protecting American interests abroad, witnesses said they saw a need for more frequent, more accurate and more timely data exchanges between Federal agencies to keep pace with the dynamic criminal and terrorist threats to U.S. citizens and corporate facilities. In this hearing, we ask whether ADNET/NCI or a program like it can meet that need. And we ask what legal organizational and fiscal barriers stand in the way of broader, more effective data-sharing.

Strengthening national security, particularly border security against dispersed but deadly criminals and terrorists requires interagency cooperation and coordination on an unprecedented scale. Data matches between Federal agencies today are often the product of good luck and the happenstance of personal relationships. The modern threat demands a more systematic collection and dissemination of the information needed to identify suspects or prevent felony criminals from entering the United States, consistent with the privacy rights and the protection of civil liberties.

Joining us today are representatives from the Department of Justice, the Secret Service, the Defense Information Systems Agency and the Department of State to describe the status of interagency data-sharing and discuss the obstacles they face in using information technology to enhance national security.

The subcommittee appreciates, truly appreciates, the contributions of our witnesses today and we look forward to their testimony.

[The prepared statement of Hon. Christopher Shays follows:]

DAN BURTON, INDIANA
CHAIRMAN

BENJAMIN A. GILMAN, NEW YORK
CONSTANCE A. MORELLA, MARYLAND
CHRISTOPHER SHAYS, CONNECTICUT
ILEANA ROS-LEHTINEN, FLORIDA
JOHN M. McHUGH, NEW YORK
STEPHEN HORN, CALIFORNIA
JOHN L. MICA, FLORIDA
THOMAS M. DAVIS, VIRGINIA
MARK E. SOUDER, INDIANA
JOE SCARBOROUGH, FLORIDA
STEVEN C. LATOURETTE, OHIO
BOB BARR, GEORGIA
DAN MILLER, FLORIDA
DOUG OSE, CALIFORNIA
RON LEWIS, KENTUCKY
JO ANN DAVIS, VIRGINIA
TODD RUSSELL PLATTS, PENNSYLVANIA
DAVE WELDON, FLORIDA
CHRIS CANNON, UTAH
ADAM H. PUTNAM, FLORIDA
C.L. "BUTCH" OTTER, IDAHO
EDWARD L. SCHROCK, VIRGINIA

ONE HUNDRED SEVENTH CONGRESS

Congress of the United States
House of Representatives

COMMITTEE ON GOVERNMENT REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515–6143

MAJORITY 202 225-5074
FACSIMILE 202 225-3974
MINORITY 202 225-5051
TTY 202 225-6852

www.house.gov/reform

HENRY A. WAXMAN, CALIFORNIA
RANKING MINORITY MEMBER

TOM LANTOS, CALIFORNIA
MAJOR R. OWENS, NEW YORK
EDOLPHUS TOWNS, NEW YORK
PAUL E. KANJORSKI, PENNSYLVANIA
PATSY T. MINK, HAWAII
CAROLYN B. MALONEY, NEW YORK
ELEANOR HOLMES NORTON,
DISTRICT OF COLUMBIA
ELIJAH E. CUMMINGS, MARYLAND
DENNIS J. KUCINICH, OHIO
ROD R. BLAGOJEVICH, ILLINOIS
DANNY K. DAVIS, ILLINOIS
JOHN F. TIERNEY, MASSACHUSETTS
JIM TURNER, TEXAS
THOMAS H. ALLEN, MAINE
JANICE D. SCHAKOWSKY, ILLINOIS
WM. LACY CLAY, MISSOURI

BERNARD SANDERS, VERMONT
INDEPENDENT

SUBCOMMITTEE ON NATIONAL SECURITY, VETERANS AFFAIRS,
AND INTERNATIONAL RELATIONS
Christopher Shays, Connecticut
Chairman
Room B-372 Rayburn Building
Washington, D.C. 20515
Tel: 202 225-2548
Fax: 202 225-2382
E-mail: hr.groc@mail.house.gov

Statement of Rep. Christopher Shays
July 24, 2001

In 1996, President Clinton declared international crime a threat to national security and ordered federal agencies to integrate and coordinate their efforts against global crime syndicates. In response, the Department of Justice (DoJ) launched the Anti-Drug Network/Nigerian Crime Initiative (ADNET/NCI), the first data-sharing project allowing all participating federal law enforcement agencies to pool active criminal case information on a secure computer network. It was hoped this initiative would help meet the threats of money laundering, narcotics trafficking and terrorism, and serve as a prototype for more efficient database coordination and cooperation.

But now it appears the ADNET/NCI project has lost momentum, falling prey to jurisdictional disputes, unresolved legal issues, bureaucratic inertia, budget constraints and personnel turnover. A key leadership position in the program has been vacant for months. What were once regular Working Group meetings have become sporadic. A number of ADNET/NCI Task Force sites appear to lack agency support.

During our hearing last April on protecting American interests abroad, witnesses said they saw a need for more frequent, more accurate and more timely data exchanges between federal agencies to keep pace with dynamic criminal and terrorist threats to U.S. citizens and corporate facilities. In this hearing, we ask whether ADNET/NCI, or a program like it, can meet that need. And we ask what legal, organizational and fiscal barriers stand in the way of broader, more effective data sharing.

Strengthening national security, particularly border security, against dispersed but deadly criminals and terrorists requires interagency cooperation and coordination on an unprecedented scale. Data matches between federal agencies today are often the product of good luck and the happenstance of personal relationships. The modern threat demands a more systematic collection and dissemination of the information needed to identify suspects or prevent known criminals from entering the United States, consistent with privacy rights and the protection of civil liberties.

Joining us today are representatives from the Department of Justice, the Secret Service, the Defense Information Systems Agency and the Department of State to describe the status of interagency data sharing efforts and to discuss the obstacles they face in using information technology to enhance national security. The Subcommittee appreciates the contributions of our witnesses today, and we look forward to their testimony.

Mr. SHAYS. We have one panel today. Our panel consists of four participants: Bruce Swartz, Deputy Assistant Attorney General, Criminal Division, U.S. Department of Justice; Mr. Bruce Townsend, Special Agent in Charge of the Financial Crimes Division, U.S. Secret Service; Ms. Catherine Barry, Director, Consular Affairs Visa Services, U.S. Department of State; and Colonel Mike Deacy, U.S. Air Force, Assistant Deputy Director, Information Engineering, Defense Information Systems Agency.

And as you are aware, we swear in our witnesses. We invite you to stand and raise your right hands.

[Witnesses sworn.]

Mr. SHAYS. I will note for the record that all of our witnesses have responded in the affirmative. I think what we will do is, we'll take you in the order that I called you.

And so you understand, the clock, we do 5 minutes and then roll over into the next 5 minutes. That is acceptable. If you get to the second red light, all hell breaks loose.

STATEMENTS OF BRUCE C. SWARTZ, DEPUTY ASSISTANT ATTORNEY GENERAL, CRIMINAL DIVISION, U.S. DEPARTMENT OF JUSTICE; BRUCE TOWNSEND, SPECIAL AGENT IN CHARGE, FINANCIAL CRIMES DIVISION, U.S. SECRET SERVICE; CATHERINE BARRY, DIRECTOR, CONSULAR AFFAIRS VISA SERVICES, ACCOMPANIED BY JOHN BRENNAN, VISA OFFICE, INTERAGENCY AND SYSTEMS LIAISON DIVISION, U.S. DEPARTMENT OF STATE; AND COLONEL MIKE DEACY, USAF, ASSISTANT DEPUTY DIRECTOR, INFORMATION ENGINEERING, DEFENSE INFORMATION SYSTEMS AGENCY

Mr. SWARTZ. Thank you, Mr. Chairman. With that warning in mind, I would like to submit my statement for the record with the subcommittee's permission.

Mr. Chairman, I appreciate the opportunity to testify this morning on behalf of the Department of Justice on the issues of interagency data-sharing and national security. My testimony this morning focuses on two distinct but interrelated topics, the Nigerian Organized Crime Initiative and ADNET, the Anti-Drug Network. We'll turn first to the Nigerian Organized Crime Initiative.

Mr. Chairman, as you noted in your opening statement, the Nigerian Organized Crime Initiative is part of the Federal law enforcement response to international organized crime. As the subcommittee is well aware, international organized crime is a rising threat to U.S. citizens. It reaches out and touches American citizens in a number of ways.

International organized crime has drawn upon the forces that have made globalization possible, including advanced telecommunications networks of travel and means of moving quickly from one country to another. In recognition of this, again as you recognized, Mr. Chairman, in your opening statement, PDD–42, has denominated international organized crime not simply as a law enforcement problem, but as a national security threat.

Mr. SHAYS. Can you suspend a second?

Can I ask if you can hear in the back? It might be such a good system it does not sound like a system. Sorry to interrupt.

Since I have already interrupted you, let me just welcome Mr. Kucinich. And I think you have a statement that you would like submitted for the record.

And if I you don't mind, as well, I am going to—to just take care of two business issues so I don't forget them. I ask unanimous consent that all members of the subcommittee be permitted to place an opening statement in the record, and that the record remain open for 3 days for that purpose. Without objection so ordered.

As for procedures, now that all witnesses be permitted to include their written statements. Without objection, so ordered.

Mr. Swartz, sorry to interrupt you. But you have the floor again.

Mr. SWARTZ. Then let me turn back to PDD–42.

Mr. SHAYS. Sure.

Mr. SWARTZ. That decision directive required that Federal law enforcement consider more interagency data-sharing, think how they could work together, how national law enforcement can work together more effectively. One part of the response to that directive was the creation of the Nigerian Organized Crime Initiative.

I want to emphasize from the outset that the focus of this initiative is not, of course, on the millions of law-abiding Nigerians both in this country and abroad. Rather, the focus is on Nigerian criminal groups that now dominate crime emanating from West Africa.

Crime arising from those Nigerian criminal enterprises has escalated over the past decade. Those criminal groups are polymorphic in nature. They engage in a wide range of crimes ranging from narcotics trafficking to alien smuggling to financial crime. Because of the wide range of their criminal activities, and the shifting membership of their groups, their loose affiliations, a number of Federal law enforcement agencies are involved in the response to Nigerian organized crime.

As Mr. Townsend of the Secret Service will explain in greater detail, since the late 1980's, the U.S. Secret Service has sponsored a number of task forces to respond to the problem of financial crime that is committed by Nigerian organized crime groups.

In 1996, following PDD–42, the Department of Justice, the Department of Treasury and the Department of State, along with the U.S. Postal Service, began to work together to develop the Nigerian Organized Crime Initiative. The principal components of that initiative are: interagency and multilateral task forces to investigate Nigerian organized crime both here and abroad; second, coordinated efforts to educate the public as to Nigerian organized crime, particularly financial crime; and, third, increased data-sharing among the Federal law enforcement agencies involved in the fight against Nigerian organized crime, including data-sharing through electronic computerized means on ADNET wanted the subcommittee's permission.

I'll now turn to the second topic that we are visiting this morning, ADNET, which is the Anti-Drug Network. As the subcommittee is aware, ADNET is a secure network administered by the Defense Information Services Agency [DISA], on DISA's Defense Information Systems network.

ADNET was established pursuant to the Defense Authorization Act of 1989 for purposes of integrating the command, control, com-

munications, and technical intelligence aspects of the United States dedicated to the interdiction of illegal drugs.

ADNET thus preexists and predates the Nigerian Organized Crime Initiative, and its scope extends beyond that initiative. By the same token, the Nigerian Organized Crime Initiative extends beyond ADNET. They are, if you will, two noncongruent circles that intersect at a certain point, that point, the area of overlap, is the use of ADNET for the use of electronic sharing of information involving Nigerian organized crime groups.

But, again, it is important to recognize that the initiative and ADNET exist independently of each other.

In April 1998, former Attorney General Reno requested that DISA agree to create, as a pilot project, the use of ADNET to share information involving Nigerian organized crime groups. It was envisioned that ADNET would serve as a secure means of exchanging information in the data bases of the various law enforcement agencies fighting Nigerian organized crime, to share, to communicate with each other as to the investigations they are conducting.

That network has grown significantly since its inception. Currently, ADNET has more than 1.5 million records involving Nigerian organized crime in its data base. That is drawing from 15 distinct data bases supplied by eight Federal agencies; 331 agents and other personnel have been cleared for access to these records.

A total of 16 ADNET network stations have been installed in six of the interagency task force offices, as well as there are two locations abroad now that have ADNET terminals that are supported by the Nigerian Crime Initiative, one in Ghana and one in Nigeria.

There are another 15 ADNET terminals in place in agency headquarters and various law enforcement field offices. At the current time, this system, that is, the Nigerian records system on the ADNET, receives approximately 1,000 queries per month as of this current year.

The chairman's letter to the Department of Justice asked for reports regarding the success of the ADNET/NCI, Nigerian Crime Initiative. This is a difficult topic to address simply because the use of ADNET and the exchange of information varies significantly from agency to agency depending upon their needs at a particular time.

Nonetheless, it is important to recognize that the Nigerian Organized Crime Initiative as a whole has registered a number of significant successes, in part because of the interagency data-sharing that has gone forward both through ADNET and other means. And Mr. Townsend will, I think, report on some of the successes that task forces and other portions of the combined initiative have tallied thus far.

We have also been asked to comment on the Department of Justice's plans for the future of the ADNET Nigerian Organized Crime Initiative in regard—again, it is important to distinguish between the Nigerian Organized Crime Initiative and ADNET; both must be assessed independently.

The Nigerian Organized Crime Initiative, again, as I have said previously, has, we believe, scored significant successes. That initiative is broader than the use of ADNET and will certainly continue in its use of task forces and information sharing.

Similarly, ADNET, again as I have pointed out, is broader than the initiative itself. And the use of ADNET for law enforcement purposes also will continue, both, we believe, within the initiative itself and outside of that initiative, since ADNET provides a secure means for law enforcement agencies to communicate with each other and provides a means for accessing other law enforcement data bases that are preexisting.

The administration will consider what steps are appropriate next to take with regard to the Nigerian Organized Crime Initiative and its use of ADNET. The possibilities include an expanded use of ADNET not only for Nigerian organized crime, but possibly for other organized crime activities.

Alternatively, there is the possibility of the use of ADNET as more of a pointer or index system. Instead of creating case data bases in each agency that can be accessed by ADNET, which is very resource-intensive, to try to use more easily uploaded sets of documents to make ADNET a means of having a broader index system.

The Department will be happy to report back after that review has taken place.

Finally, we have been asked to talk some on the legal and other options——

Mr. SHAYS. We'll come back. You have had 10 minutes.

Mr. SWARTZ. Thank you.

Mr. SHAYS. I think you were curious to see what would happen with the red light. I was sure that you wouldn't point out that I was a fraud.

I also like put the fear in you. It accomplished nothing.

Mr. SWARTZ. No. I am very fearful actually.

[The prepared statement of Mr. Swartz follows:]

Department of Justice

STATEMENT

OF

BRUCE C. SWARTZ
DEPUTY ASSISTANT ATTORNEY GENERAL
CRIMINAL DIVISION

BEFORE THE

SUBCOMMITTEE ON NATIONAL SECURITY, VETERANS AFFAIRS,
AND INTERNATIONAL RELATIONS
COMMITTEE ON GOVERNMENT REFORM
UNITED STATES HOUSE OF REPRESENTATIVES

CONCERNING

FEDERAL INTERAGENCY DATA SHARING AND NATIONAL SECURITY

PRESENTED ON

JULY 24, 2001

Opening Statement by Bruce C. Swartz
Deputy Assistant Attorney General
Criminal Division, Department of Justice

Before the Subcommittee on National Security,
Veterans Affairs, and International Relations
Committee on Government Reform and Oversight
House of Representatives
July 24, 2001

Good morning, Mr. Chairman, and Members of the Subcommittee. I appreciate this opportunity to testify before you this morning on behalf of the Justice Department on federal inter-agency data-sharing and national security. I want to thank the Chairman and the Subcommittee's staff for identifying in advance some of the Subcommittee's particular areas of interest. In keeping with that guidance, I will focus my prepared remarks on the Department's experience with the Nigerian Organized Crime Initiative (NCI)and the Anti-Drug Network (ADNET).

As you requested, I will begin with a brief overview of NCI and ADNET.

Overview of ADNET/NCI:

The Department of Justice's participation in the ADNET/NCI system grows out of the Department's overall response to the threat of international crime.

As this Subcommittee is well aware, international crime is a serious and growing threat to our national security. Organized crime groups have been quick to take advantage of new criminal opportunities created by the globalization of business and financial activity, dramatic increases in international travel, and revolutionary advances in technology and communications. International criminal networks engage in a broad range of criminal activities that directly affect the United States and its citizens, including narcotics trafficking, alien smuggling, terrorism, mail and wire fraud, financial crimes, money laundering, and various types of cybercrime, such as hacking, identity theft and child pornography.

In 1995, Presidential Decision Directive 42 (PDD-42)concluded that international crime presents a serious threat to our national security. PDD-42 ordered agencies of the executive branch of the U.S. government to increase the priority and resources devoted to addressing international crime. It also called for more effective internal, interagency and international coordination.

The Justice Department has responded by working within the federal law enforcement community to increase cooperative efforts against international crime, with particular emphasis on priority

threats such as those presented by organized international criminal and terrorist groups.

The inter-agency initiative against crime committed by international criminal groups operating out of Nigeria and other West African countries is one part of a broad Departmental and Executive Branch initiative to enhance inter-agency cooperation across the board on international crime control, especially on policy and programmatic issues. Crime emanating from these groups has been escalating over the past decade. Because a large number of law enforcement agencies have been involved in fighting various aspects of Nigerian organized crime, it is an area where the potential benefits of inter-agency cooperation and coordination appeared high.

Nigerian criminal groups are known to engage in a broad range of criminal activity, including: narcotics trafficking, especially heroin and cocaine; financial crimes; money laundering; immigration fraud; corruption; and alien smuggling. Experience has shown that Nigerian criminal enterprises are usually involved in more than one type of criminal activity. Nigerian criminal organizations also tend to be non-hierarchical and adaptable, with large numbers of criminal entrepreneurs operating in loose associations with established organizations.

This structure often frustrates traditional single-agency law enforcement methods.

I want to emphasize from the outset that the focus of the Nigerian Organized Crime Initiative is not on the millions of law abiding Nigerians, here and abroad. Rather, our focus is on Nigerian criminal groups that now dominate crime emanating from West Africa.

In response to the special challenge presented by Nigerian crime, law enforcement components from the Departments of Justice, Treasury, and State, along with the United States Postal Service, have worked together to develop the Nigerian Organized Crime Initiative. The principal components of the NCI are:

(1) interagency and multilateral working groups and task forces to address crime problems arising from Nigerian criminal enterprises, including regional inter-agency task forces, hosted by the United States Secret Service field offices in nine major U.S. cities;

(2) coordinated efforts to educate the public regarding the criminal activities of Nigerian criminal enterprises;

(3) systems, including ADNET, to facilitate the substantive exchange of information within the law enforcement community and the use of such information to help identify targets for investigation; and

(4) the use of joint national and international investigations.

In April of 1998, at the request of former Attorney General Janet Reno, the Defense Information Systems Agency agreed to create, as a pilot project, a discrete law enforcement database for the Nigerian Organized Crime Initiative on ADNET, which is a secure DISA-administered communication network used primarily by the military and the intelligence community.

It was envisioned that ADNET would provide a secure and efficient means for the task forces, agency headquarters and overseas locations to share law enforcement information. The network has grown significantly since its inception.

Currently, the ADNET/NCI system contains more than 1.5 million records, drawn from 15 databases supplied by 8 federal law enforcement agencies. 331 agents and other personnel have been cleared for access to the system. A total of 16 ADNET workstations have been installed in six of the Interagency

Nigerian Organized Crime Task Force offices; five others are operating in overseas locations, and another 15 are in place in agency headquarters or field offices. The system currently averages more than 1000 queries per month. Among Justice Department components, the Immigration and Naturalization Service is the heaviest user.

Successful applications of ADNET/NCI data in criminal cases:

The Chairman's letter to the Attorney General concerning this hearing asked about successful applications of ADNET/NCI data in criminal cases. The Department's experience with the database has been mixed. The perceived value of the ADNET/NCI system varies among Justice Department components. For example, the INS has found the ability of the system to securely communicate sensitive data to be highly valuable. INS has also successfully used the system to obtain information that has led to the apprehension of fugitives. For other Justice agencies, however, such as the DEA and the FBI, which have more robust internal databases and access to alternative secure communications networks, the marginal value of the ADNET/NCI system, at least to date, has been more modest. It is clear that the ability of the system to produce successful applications in criminal cases is largely dependent on two factors: (1) the

quality and quantity of law enforcement information inputted; and (2) the number of relevant criminal investigators with ready access to that information.

DOJ program plan for ADNET/NCI, to include national security applications:

The Department's future plans for the ADNET/NCI pilot project and the possible expansion of the ADNET system into other areas are still undetermined. In this regard in particular, it is important to distinguish between NCI and ADNET. ADNET has numerous potential uses for law enforcement, including secure communications, and access to preexisting databases, such as EPIC and NDIC. NCI is thus only one possible use for ADNET. The new Administration, including the incoming leadership at the major DOJ law enforcement agencies, has not yet had an opportunity to review the NCI pilot project and make a decision as to its future. Among the questions that might be considered are whether it is cost effective to continue to use ADNET to focus on Nigerian crime, or whether other alternatives might offer greater efficiency. More generally, the new Administration will consider whether the ADNET/NCI initiative should be expanded to include other types of organized crime, or whether other forms of information sharing - such as using ADNET to access preexisting

databases - might be a better alternative. The Department would be happy to report back to the Subcommittee once such a review is completed.

Legal, financial and administrative issues affecting interagency data-sharing:

There are a host of legal, financial and administrative issues that affect interagency data-sharing. Depending on why the data was originally collected, who will have access to it and for what purpose, there may be many categories of information that must be excluded from an inter-agency data base, or to which access must be highly limited. These restrictions may be the result of legal requirements like the Grand Jury secrecy provisions of Rule 6(e), the Privacy Act, or federal statutes governing electronic surveillance, or they may be the result of sensitive law enforcement interests, such as protecting the identify of a confidential source.

Reviewing and redacting investigative documents before they are entered into a shared database is a time-consuming, resource intensive undertaking, which can divert agent and support staff resources from on-going investigations.

Review of the "lessons learned" during the implementation of ADNET/NCI:

As for lessons learned from our experience from ADNET/NCI, a definitive list of specific lessons will have to wait until the Department's leadership has had an opportunity to gather and review various internal impressions of the system. I can offer the following lessons learned at this time:

1. Interagency cooperation, including the sharing of law enforcement information is often critical for the successful investigation and prosecution of international organized crime, including Nigerian organized crime.

2. Cooperation and coordination with foreign counterparts are also essential.

3. ADNET/NCI is one of many potentially effective ways to share data and coordinate law enforcement efforts.

4. Developing a database like ADNET/NCI is a challenging, resource intensive undertaking.

5. The value of ADNET/NCI to a particular law enforcement agency can vary significantly depending on the mission of that agency.

6. The costs and benefits of ADNET/NCI need to be carefully considered.

7. There is a tension between ease of use and security.

8. To a certain extent there is a "chicken and the egg" problem with a database like ADNET/NCI. The system cannot be useful unless agencies make a commitment to invest resources to load important data. But agencies are reluctant to commit resources to data entry until the system can demonstrate its usefulness.

9. Without a substantial, high level commitment, inter-agency data sharing systems are unlikely to overcome this "chicken and egg" problem.

Mr. Chairman, thank you. I would be happy to answer any questions that you or other members of the Subcommittee may have.

Mr. SHAYS. Mr. Townsend.

Mr. TOWNSEND. Mr. Chairman, thank you for the opportunity to address the subcommittee on the subject of Federal interagency data-sharing and the Secret Service's role in the Anti-Drug Network/Nigerian Crime Initiative. I have prepared a comprehensive statement which will be submitted for the record. With the subcommittee's permission, I will summarize it at this time.

Mr. SHAYS. Sometimes the summary is longer than the statement.

Mr. TOWNSEND. I will endeavor to make sure that is not the case.

Mr. SHAYS. We want you to cover the territory, so you go ahead.

Mr. TOWNSEND. In addition to providing the highest levels of physical protection to our Nation's leaders, the Secret Service exercises broad investigative jurisdiction over a variety of financial crimes. As the original guardian of our nation's financial payment system, the Secret Service has a long history of pursuing those who would victimize our financial institutions and law-abiding citizens.

In recent years, a combination of the information technology revolution and the effects of globalization have caused the investigative mission of the Secret Service to evolve in a manner that cannot be overstated.

With the passage of the Omnibus Crime Control Act of 1984, the Secret Service was provided jurisdiction to investigate access device fraud. One of the first groups that the Secret Service identified as being heavily involved in this crime was a loosely organized criminal element within the growing Nigerian population in the United States.

It is important to emphasize at the outset that despite the Nigerian criminal elements that now dominate crime emanating from West Africa, we in the Secret Service recognize that there are millions of law-abiding Nigerians at home and abroad whose rich tradition and culture we admire and whose contributions to our society we value.

The democratically elected government that came to power in Nigeria in 1999 is keenly aware that the extensive involvement by Nigerians in financial scams carried out around the world and in the international drug trade creates not only enormous financial losses, but often feeds widespread, but unjustified, perceptions about Nigerians. Nigeria still retains many legitimate opportunities for business and investment; however, there are corporations around the world that are reluctant to deal with Nigerian companies for fear of becoming embroiled in fraudulent activity.

Only by sharing our combined expertise and resources will we be able to effectively address the Nigerian organized crime problem that plagues us all.

In the late 1980's, the Secret Service took a proactive approach to combating Nigerian organized crime by establishing and maintaining task forces throughout the United States whose main focus was the investigation of financial fraud committed by Nigerian nationals and their accomplices. Membership in these task forces included representatives from the U.S. Customs Service, the Immigration and Naturalization Service, the U.S. Postal Inspection Service, the DEA, the FBI, the IRS, the Department of State's Bureau of Diplomatic Security, bank investigators from the private

sector, as well as numerous State and local law enforcement agencies.

In May 1996, pursuant to PDD–42, a Federal law enforcement interagency working group was created to develop a domestic law enforcement strategy regarding Nigerian organized crime. The strategy that was developed targeted both domestic and international Nigerian criminal activity, and emphasized coordination of U.S. law enforcement, the sharing of investigative leads and information and enhanced cooperation with our foreign law enforcement counterparts to coordinate multinational cases and investigations.

The proposed enforcement efforts of this strategy became known as the Nigerian Crime Initiative. The working group also proposed to utilize its computer data base to share Nigerian case data electronically. It was later agreed that the Department of Defense Information Systems Agency Anti-drug Network, ADNET, would be the mechanism for sharing this information.

In an effort to take the fight against these criminal organizations to its source, on January 12, 1999, the Secret Service began a cooperative effort with the U.S. Embassy in Nigeria and the Nigerian National Police. The purpose of this effort was to provide operational, investigative and training assistance to the NNP and other Nigerian Federal law enforcement agencies. A task force was established in Lagos, Nigeria, that was initially staffed by two special agents of the Secret Service on rotating temporary assignments.

Over the next 16 months, using information supplied by the 11 domestic task force, the Secret Service assisted the NNP in executing search warrants at more than 100 suspected advance fee fraud plants around Lagos, which, in turn, resulted in nearly 200 arrests.

The challenge we face is great, but the progress we are making against Nigerian criminal elements is positive, as is the commitment by the new democratically elected government in Nigeria to become a full partner in these efforts.

Mr. Chairman, that concludes my prepared statement. I would be happy to answer any questions.

Mr. SHAYS. Thank you, Mr. Townsend.

[The prepared statement of Mr. Townsend follows:]

U.S. Secret Service

Testimony of Mr. Bruce A. Townsend
Special Agent in Charge - Financial Crimes Division

Before

The Subcommittee on National Security, Veterans Affairs, and International Relations
House Committee on Government Reform
U.S. House of Representatives

July 24, 2001

Mr. Chairman, members of the Subcommittee, thank you for the opportunity to address the Subcommittee on the subject of federal interagency data-sharing and the Secret Service's role in the Anti-Drug Network/Nigerian Crime Initiative.

In addition to providing the highest level of physical protection to our nation's leaders, the Secret Service exercises broad investigative jurisdiction over a variety of financial crimes. As the original guardian of our nation's financial payment systems, the Secret Service has a long history of pursuing those who would victimize our financial institutions and law-abiding citizens. In recent years, the combination of the information technology revolution and the effects of globalization have caused the investigative mission of the Secret Service to evolve in a manner that cannot be overstated.

With the passage of the Omnibus Crime Control Act of 1984, the Secret Service was provided jurisdiction to investigate access device fraud. One of the first groups that the Secret Service identified as being heavily involved in this crime was a loosely organized criminal element within the growing Nigerian population in the United States.

It is important to emphasize from the outset that despite the Nigerian criminal elements that now dominate crime emanating from West Africa, we in the Secret Service recognize that there are millions of law-abiding Nigerians, at home and abroad, whose rich tradition and culture we admire and whose contributions to our society we value.

The democratically-elected government that came to power in Nigeria in 1999 is keenly aware that the extensive involvement by Nigerians in financial scams carried out around the world, and in the international drug trade, creates not only enormous financial losses, but also feeds widespread, but unjustified, perceptions about Nigerians. Nigeria still retains many legitimate opportunities for business and investment. However, there are corporations around the world that are reluctant to deal with Nigerian companies for fear of becoming embroiled in fraudulent activity. It is simply unfair that the activities of these criminal elements negatively impacts the economic potential of Nigeria. Only by sharing our combined expertise and resources will we be able to effectively address the Nigerian organized crime problem that plagues us all.

In the late 1980s, the Secret Service took a proactive approach to combating Nigerian organized crime by establishing and maintaining task forces throughout the United States whose main focus was the investigation of financial fraud committed by Nigerian nationals and their accomplices. Membership in these task forces included representatives from the United States Customs Service, the Immigration and Naturalization Service, the United States Postal Inspection Service, the Drug Enforcement Administration, the Federal Bureau of Investigation, the Internal Revenue Service, the Department of State's Bureau of Diplomatic Security, bank investigators from the private sector, as well as numerous state and local law enforcement agencies. This diverse membership is indicative of the multitude of crimes being perpetrated by Nigerian criminals.

These crimes include credit card fraud, bank fraud, check kiting, various types of insurance fraud, entitlement fraud, false identification, passport and visa fraud, marriage fraud to obtain U.S. citizenship, vehicle thefts, the counterfeiting of U.S. currency, and the counterfeiting of corporate checks and other obligations. These attacks on our nation's financial systems usually involve careful planning, a precise execution of the scheme, and often focus on taking advantage of financial systems designed to be consumer or customer friendly.

Nigerian advance fee fraud, also known as "4-1-9 fraud" after a section of the Nigerian criminal code, has emerged as one of the most lucrative fraudulent activities perpetrated by organized criminal elements within the Nigerian community. Worldwide financial losses associated with advance fee frauds are conservatively estimated in the hundreds of millions of dollars annually, with victims in the United States accounting for a significant percentage of the total.

Experience has shown that seldom, if ever, are these enterprises engaged in one form of criminal activity to the exclusion of other types of crime. These organizations are responsible for financial crimes and fraud schemes costing Americans, and citizens of countries around the world, hundreds of millions of dollars a year, as well as for the importation of a significant amount of the heroin used in the United States, and much of the cocaine smuggled to Europe, Asia and Africa.

Nigerian criminal enterprises have proven to be particularly adept at taking advantage of opportunities created by the combined effects of globalization and the information technology revolution. They are now engaged in a broad range of criminal activities that reach across borders and victimize citizens, businesses and financial institutions in Africa, Europe, Canada, the United States and around the world. Nigerian criminal enterprises present unique challenges to law enforcement because their organizational structures and criminal activities are so varied.

Nigerian criminal groups are highly fluid in personnel and in methods of operation. Although there is a degree of structure to these organizations, their hierarchical composition and relationships are not comparable to those of more traditional criminal organizations. In terms of structure, these enterprises seem to range from independent entrepreneurs to highly organized syndicates. These groups are able to change and adapt as needed, both in the nature of the criminal activities they pursue, and in the members they employ. This flexibility allows them to remain in operation and to insulate themselves from law enforcement. The only viable means of

attacking these groups is through a multi-agency or task force approach, while also finding ways to better share criminal intelligence information.

Although crimes committed by groups of Nigerians may seem unrelated, connections and patterns are being developed in criminal activities from credit card fraud to drug smuggling, and from identity theft to money laundering. The speed with which some of these groups react to enforcement efforts and adopt new techniques demonstrates the effectiveness of their inter-group intelligence sharing and the coordination between the various syndicates. If we are to be successful, it is critical that we in law enforcement share information and coordinate our efforts as effectively as the syndicates we investigate.

On October 21, 1995, Presidential Decision Directive 42 (PDD-42) was issued, directing government agencies to increase the level of resources devoted to combating international organized crime, to achieve greater effectiveness by improving the coordination of federal law enforcement efforts, to work more closely with other governments to develop a global response to this threat, and to aggressively and creatively use all legal means to combat international crime. In response to PDD-42, the Attorney General directed federal law enforcement to increase their cooperative efforts against international organized crime, including Nigerian organized crime.

In May of 1996, pursuant to PDD-42, a federal law enforcement interagency working group was created to develop a domestic law enforcement strategy regarding Nigerian organized crime. The strategy that was developed targeted both domestic and international Nigerian criminal activity, and emphasized increased coordination of U.S. law enforcement, the sharing of investigative leads and information, and enhanced cooperation with our foreign law enforcement counterparts to coordinate multinational cases and investigations. Moreover, by improving coordination and dialogue with the government of Nigeria, especially Nigerian law enforcement officials, this strategy strengthened their ability to combat crime occurring within Nigeria, and assist in combating crimes committed elsewhere in the world by individuals and organizations located in Nigeria. The proposed enforcement effort of the strategy became known as the Nigerian Crime Initiative (NCI).

The working group also proposed to utilize a computer database to share Nigerian case data electronically. It was later agreed that the Department of Defense/Defense Information Systems Agency's Anti-Drug Network (ADNET) would be the mechanism for sharing this information. ADNET uses web-based technologies and a classified communication system to enable participants to securely exchange data.

In 1998, then-Attorney General Reno approved the recommendation of the working group to establish the Interagency Nigerian Organized Crime Task Force (INOCTF). Additionally, it established the installation of the ADNET-NCI system to support these task forces and selected foreign sites.

It was recognized by the interagency working group that the Secret Service had been combating criminal issues related to Nigerian organized crime prior to the creation of the working group in

1996. The Secret Service had hosted existing task forces designed to combat aspects of Nigerian organized crime—specifically that of access device fraud—since the late 1980s.

It was agreed by the Attorney General and participants of the interagency working group that existing Secret Service Nigerian Task Forces would evolve into new Interagency Nigerian Organized Crime Task Forces (INOCTFs). Additionally, these task forces would continue to be hosted by the Secret Service. It was also agreed that the creation of future task force sites and the agency-host of these sites would be determined at the discretion of the interagency working group.

Accordingly, Secret Service hosted INOCTFs were established from existing Secret Service Nigerian Crime task forces located in New York, Newark, Chicago, Houston and Atlanta. The process of installing ADNET terminals for these offices began in early 1998 and was completed in late 1999.

Since the inception of NCI, other task forces have been established in Dallas and Washington, DC. Proposed NCI task force sites include Baltimore and Los Angeles. Overseas, ADNET terminals have been installed at the U.S. Consulates in Lagos, Nigeria, and Accra, Ghana. These overseas terminals help to further the law enforcement efforts waged against Nigerian organized crime in those countries. Additional terminals have been installed at the headquarters of most of the participating agencies involved with NCI.

The Secret Service provides the following resources as host to a task force:

- A full-time Criminal Research Specialist (CRS), trained in the use of the ADNET terminal, is assigned directly to each task force. This individual acts as a point-of-contact for all participating task force personnel. The CRS can provide information obtained from ADNET to all law enforcement participants assigned to the task force.

- Task force space is also provided. Each task force site must follow strict security regarding the housing of each ADNET terminal. Each site must also allow independent access to members of each participating agency twenty-four hours a day, seven days a week.

It has been the experience of the Secret Service that the criminal groups involved in financial crimes routinely operate in a multi-jurisdictional environment. By working closely with other federal, state, and local law enforcement officials, as well as international police agencies, we have been able to jointly develop a comprehensive network of intelligence sharing, resource sharing, and technical expertise that bridges jurisdictional boundaries. Moreover, the use of a classified, secure communication system, and its attendant regulations and protections, furthers the goal of safeguarding the privacy of citizens.

These task forces have had success in disrupting the access device and bank fraud activities of these groups, and have even been able to affect ongoing advanced fee fraud schemes, demonstrated by recent investigations in New York. In two separate undercover investigations, meetings were arranged in which members of the INOCTF, posing as Nigerian advance fee fraud victims, met with suspects who were perpetrating a "black money" scam. In one such meeting,

the "sales pitch" of the suspects, and their demonstration of the chemical process for removing the black substance from a genuine $100 Federal Reserve Note, was captured on video tape.

These meetings led to the arrest of four suspects on wire fraud charges. Subsequently, two federal search warrants were executed on a residence and a storage locker used by another suspect, who was thought to control the majority of the advanced fee fraud activity in the New York metropolitan area, particularly "black money" scams. Extensive documentary and electronic evidence was seized, including volumes of victim information and four footlocker style trunks containing approximately one thousand pounds of "black money." A review of the recovered documents has enabled INOCTF members to link eight defendants from other advanced fee fraud related cases to this suspect, and identified actual losses in excess of $3 million.

Despite such successful investigations by the INOCTF, lasting success in dismantling the advanced fee fraud operations of Nigerian criminal enterprises has been much more elusive. One problem has been that advanced fee fraud schemes originate in Nigeria and other West African countries with letters, faxes, and e-mails, and the suspects defraud U.S. citizens without ever entering the United States. This is accomplished by either conducting all of the "business" by telephone, fax, mail, e-mail, and wire, or by having face-to-face meetings in Canada, the United Kingdom, or Africa.

Interdiction efforts and consumer education initiatives have been further complicated by the evolution of the schemes themselves. Nigerian criminal enterprises have adopted new technologies and modern marketing practices more quickly than most multi-national corporations, constantly refining their delivery methods and their "pitch" to circumvent the efforts of law enforcement and consumer protection agencies.

In an effort to take the fight against these criminal organizations to its source, on January 12, 1999, the Secret Service began a cooperative effort with the U.S. Embassy in Nigeria, and the Nigerian National Police (NNP). The purpose of this effort was to provide operational, investigative and training assistance to the NNP and other Nigerian federal law enforcement agencies.

A task force was established in Lagos, Nigeria that was initially staffed by two Special Agents of the Secret Service on rotating temporary assignments. Over the next sixteen months, using information supplied by the eleven domestic task forces, the Secret Service assisted the NNP in executing search warrants at more than one hundred suspected advance fee fraud plants around Lagos, which in turn resulted in nearly two hundred arrests.

Information developed by the task force in Lagos also led to the arrests of Nigerian criminals operating within the United States, as well as the identification and seizure of the proceeds of advanced fee fraud schemes secreted in financial institutions in the United States. Due to the overwhelming success of this initiative, as well as the support of the U.S. Embassy, the newly established U.S. Consulate, and the NNP, the Secret Service established a permanent office in Lagos in June of 2000, which has continued to build on the positive trend begun by the temporary initiative.

The Secret Service is proud of the relationships we have developed, and have continued to strengthen, with our foreign law enforcement counterparts, especially the Special Frauds Unit of the Nigerian National Police. We believe that such international partnerships are an essential component of efforts to carry out the mandate of PDD-42.

I would like to take this opportunity to commend the Department of State for their tireless and unwavering support of our efforts in Nigeria. The extensive cooperation that the Secret Service has received from the staff of the U.S. Embassy and the U.S Consulate has been instrumental in our success, as has the support of the Bureau of International Narcotics and Law Enforcement.

The challenge we face is great. But the progress we are making against Nigerian criminal elements is extremely positive, as is the commitment by the new democratically elected government in Nigeria to become a full partner in these efforts. Increased cooperation among federal, state, and local officials in the U.S., our foreign partners, international organizations, and private institutions around the world, is the only way to make an effective and united stand against transnational crime.

Mr. SHAYS. Ms. Barry.

Ms. BARRY. Thank you, Mr. Chairman. It is a pleasure to be here today to comment on the efforts of the Bureau of Consular Affairs for the Department of State to use an enhanced interagency data-share. I have prepared a written statement, and with your permission, will submit it for the record and make a few oral remarks.

Mr. SHAYS. Yes. Thank you.

Ms. BARRY. As you are well aware, sir, our visa workload overseas has grown steadily every year. In fiscal year 2000, we processed 413,000 immigrant visa cases and close to 10 million nonimmigrant visa cases. That resulted in issuing visas to the tune of 7.1 million and denying visas to 2.4 million applicants.

The visa waiver program approved by Congress last year prevented this number from growing even higher. Data-share has become essential to us, keeping up with this growing workload and providing visa adjudication in an efficient manner.

Using funding provided by the machinery to do visa fee, the Bureau of Consular Affairs installed modernized computers overseas for all visa functions, and we covered all of our operations worldwide by September 1999.

Since that time, we have continued to improve our systems, both the hardware and software. This year, our most significant achievement was the replication of all visa data in Washington in a manner that can be accessed by the Bureau of Consular Affairs and consular officers overseas.

One constant element of our efforts since 1999 has been to expand data-share with other agencies. Our Lookout System, known as CLASS-E, keeps growing, in part because of the data-share agreements we have with other agencies. Our Lookout data base now has 5.7 million records.

With regard to immigrant visa cases, we now share 55 percent of our immigrant visa data with INS and Customs at 16 ports of entry. Data on new cases is available to these agencies in less than an hour.

The Bureau of Consular Affairs, INS and the Social Security Administration have recently reached an agreement to use immigrant visa data to ensure the secure issuance of Social Security numbers to new immigrants.

With regard to nonimmigrant visa cases, earlier this month we began a pilot to share data on issued visas with INS ports of entry. The pilot program currently includes the INS operation at Newark Airport. For example, by looking at the photo in our data base, INS inspectors will be able to uncover imposters more quickly and effectively.

We maintain dialog with analysts, especially those who work on antiterrorism or antiorganized crime projects to ensure that their hard findings are captured in an appropriate visa Lookout entry. We share with INS information on lost and stolen passports.

And to sum up, in our view, the results of these efforts have been faster detection of fraud overseas, improved evidence and greater overall deterrence. We know there is always room for improvement; in this vein, we continue to improve the algorithms we use to define the search in the Lookout System on foreign names.

The comments an adjudicating officer may make in an electronic record of a specific case will soon be available to consular officers at other posts, as well as to INS inspectors.

The next projects in our horizon are a pilot program using facial recognition technology, enhanced data-share with the FBI on criminal alien records for which legislation would be required. We are talking to Customs about getting more data on serious violators. And with DEA we are discussing improving the timeliness of our connectivity.

I would like to close by reiterating that the use and enhancement of data-share is and will remain a significant objective of the Bureau of Consular Affairs. We view data-share as a means of facilitating legitimate travel and improving border security, although our focus is a little different.

Obviously, from my remarks, we are focused more on the hard findings rather than on the analytical side of the process.

Thank you, Mr. Chairman.

Mr. SHAYS. Thank you, Ms. Barry.

[The prepared statement of Ms. Barry follows:]

STATEMENT OF

CATHERINE BARRY
MANAGING DIRECTOR, VISA OFFICE
BUREAU OF CONSULAR AFFAIRS

BEFORE THE

SUBCOMMITTEE ON NATIONAL SECURITY, VETERANS AFFAIRS AND INTERNATIONAL RELATIONS

COMMITTEE ON GOVERNMENT REFORM

UNITED STATES HOUSE OF REPRESENTATIVES

July 24, 2001

Mr. Chairman and Members of the Committee:

Thank you for the opportunity to appear before you to give an overview of interagency datasharing from the perspective of the Bureau of Consular Affairs and particularly the Visa Office. I will comment on both our successes and on work that remains to be done. In response to your letter of June 29, I will focus on our automation, our interagency datasharing and the impact of datasharing on our border security.

Mr. Chairman, in fiscal year 2000, Consular Affairs continued to respond to the demands of foreign citizens to enter the United States. We issued 413,000 immigrant visas and over 7.1 million nonimmigrant visas. The Visa Waiver Program for visitors was in effect for 29 countries.

We registered slightly more than 2.4 million nonimmigrant visa refusals in FY-2000. These results underscore our careful scrutiny of nonimmigrant visa applications in response to national concern over undocumented workers seeking U.S. jobs, increasingly sophisticated attempts at visa fraud and international terrorism. A visa refusal normally requires more time than an issuance. Since consular resources are stretched thin, in part by the time-consuming task of processing refusals, we have come to rely increasingly on our modernized systems and interagency datashare to get our job done.

Beginning in 1993 with the support and interest of the Congress, the Consular Affairs Bureau modernized its visa systems. By September 1999 the Bureau had installed modernized consular applications supporting all visa functions worldwide. These new systems offer significant operational and security improvements. Now in 2001, the Bureau is reaping the harvest as Consular Affairs brings back or "replicates" all relevant visa data from the field and embarks on enhanced datashare.

Mr. Chairman, last January, following up on a November 14, 2000 briefing provided by Consular Affairs and others to your subcommittee staff, our Acting Assistant Secretary for Legislative Affairs wrote to you. In that letter, he

provided an overview of interagency datasharing. We are pleased to report further progress in our quest for effective interagency datasharing aimed at both securing our borders and facilitating the entry of legitimate travelers to our country. As we move forward, we remain mindful of the need to provide appropriate protection during the data sharing process against unauthorized disclosure of personal information and will take all necessary steps to ensure the privacy of U.S. citizens, lawfully admitted aliens, and legitimate nonimmigrant visa applicants. I'd like to comment on three areas: Immigrant Visa Datasharing, Nonimmigrant Visa Datasharing and our Consular Lookout and Support System.

Immigrant Visa Datashare Pilot

Currently Consular Affairs exchanges 55 percent of our immigrant visa data with INS and Customs at 16 U.S. ports of entry. INS primarily employs this information to complete its inspections of new immigrants. In the last year, Consular Affairs has sped up transmission of this data so that it now arrives within the targeted time frames. For example, in El Paso, Consular Affairs must get the data to the port of entry in 45 minutes, since newly approved immigrants often arrive from our Consulate General in Ciudad Juarez that quickly.

Consular Affairs plans further reform and improvement of the immigrant visa procedures. Immigrant visa reform envisions expanded immigrant visa datashare, meaning that one hundred percent of all immigrant visa data would go to INS for use in port of entry inspections and the processing of legal permanent residents' documentation. Social Security has reached agreement with Consular Affairs and INS to use immigrant visa data to ensure secure issuance of social security numbers to all immigrants. We aim to complete this exchange by the end of 2001.

Nonimmigrant Visa Datashare Pilot

Consular Affairs deployed Nonimmigrant Visa Datashare with INS on July 10, 2001. It began with limited data. INS will make the data available to several pilot ports of entry in August. Making this data available to INS inspectors will enhance their identification of legitimate travelers versus impostors. Nonimmigrant Visa Datashare gives INS access to data from our posts abroad including border-crossing card data, digitized photographs, and issuance and refusal information. We aim to get all nonimmigrant visa data to all ports of entry as soon as possible.

Consular Lookout and Support System

Prior to issuing any visa, our posts check our lookout database called the Consular Lookout and Support system. The Consular Lookout and Support System - Enhanced (CLASS-E) contains approximately 5.7 million records, most of which originate with our embassies and consulates abroad through the visa application process. INS, DEA, the Department Of Justice and other federal agencies also contribute lookouts to our system. INS provides us with about 1.17 million lookout records and DEA provides some 330,000 records. INS and the Department exchange lookout information electronically via the Treasury Enforcement Communication System (TECS), which is administered by the Customs Service and which is accessible by numerous agencies in the Interagency Border Inspection System (IBIS). Through IBIS we share about 500,000 lookouts with INS. The INR/TIPOFF program funded by Consular Affairs provides lookout information to INS on over 22,000 known or suspected terrorists and provides over 47,000 lookout records to CLASS-E.

What is the Bureau of Consular Affairs' view of the impact of datasharing on terrorism, border security and national security?

We are not here today to offer datashare as a panacea for the challenges we face on border security. We are well aware of the need for more work in this area. However interagency datasharing improvements will yield greater efficiency in handling high-risk cases. I would like to relate three effects of datasharing: faster detection of fraud, improved evidence and greater deterrence.

We have already seen examples of faster detection of mala fide and inadmissible aliens at our visa units overseas. Since May of this year, Consular Affairs shares all electronic nonimmigrant visa data with all visa units overseas. For the first time consular officers not only can check a visa case history almost "real-time" locally but also globally. Our posts have already had considerable success in detecting fraud and in facilitating legitimate travel using this tool.

Beginning in 1997, Consular Affairs started to add linguistic algorithms to the basic namecheck routines used by CLASS. The Arabic algorithm added in 1997 regularizes multiple transliterations of Arabic names. A linguistic algorithm covering the languages used in the former Soviet Union, including Turkic and Baltic languages was deployed in 2000. Work is now being done on an algorithm for Hispanic names, which account for about half of all the

queries to CLASS. A study was completed this year on algorithms for East Asian Languages, but decisions on developing algorithms for Chinese and other languages are still pending. Our current backup system to CLASS will be replaced with a successor system called the Back-up Namecheck System (BNS) in 2002. BNS will provide a back-up system that uses similar namecheck logic to the CLASS system. Strengthening CLASS will strengthen our visa units' ability to detect inadmissible aliens.

With datasharing, INS border inspectors will have faster access to Consular Affairs lookout information. We are continually enhancing CLASS and looking for additional sources of information that will allow us to do our jobs better. In 1999, we began to store information on lost and stolen blank foreign passports in CLASS. This year we started to share this information with INS at ports of entry through TECS. Using such information, both our posts and ports of entry have detected travelers carrying stolen documents. Another recent enhancement to CLASS is the capacity to receive and store extended comments. We are already receiving comments from INS records. When the next software release of the NIV system is made this year, posts will gain the ability to read these extended comments and add comments of their own. We will pass comments on

"serious violators" to IBIS. This will be a fundamental enhancement to inspectors' ability to process an inadmissible arrival more quickly.

Immigration inspectors and visa officers already identify many impostors and cases of malfeasance but with datasharing the photographic evidence is improved. With the modernization of our systems, we now replicate all nonimmigrant visa photos into a central database and can pass them to INS. We are also testing facial recognition as a tool to detect duplicate candidates for the Diversity Visa lottery. Using facial recognition we will be able to detect if some DV applicants are making improper duplicate applications. Photos help make more positive identifications of the perpetrators of fraud.

As we look ahead to fuller and more complete exchanges of immigration data, we hope to see strengthened evidence to prove inadmissibility. Consular Affairs is working with TIPOFF, INS, the FBI, Customs and DEA to improve interagency datasharing in several ways as follows:

--The Department of State and FBI have consulted and reached initial agreement on the Department's access to certain FBI criminal alien record data. Access to FBI lookout extracts would greatly assist consular officers in their adjudication of visa applications. Legislation is

required to implement this understanding. The Administration is currently working on legislation to implement this.

--Customs is taking steps to share their serious violator data with the Consular Affairs Bureau which will help us primarily to avoid issuance of visas to drug offenders previously arrested or detained by Customs, principally at the southwest border.

--Consular Affairs already exchanges data with DEA (about 330,000 records) but we want to improve the efficiency of this exchange closer to "real-time" rather than the slower tape exchange we now employ. Consular Affairs and DEA are in agreement and it is now a matter of discussion on the logistics.

--In regular consultations with INS, we are working to upgrade datashare, ensure lookout data quality and improve the speed of transmission of departure and deportation data.

--Through the TIPOFF program, funded by our Bureau and managed by the Bureau of Intelligence and Research, we will continue to monitor and develop further information on suspected terrorists numbering about 47,000 names.

We believe interagency datasharing, when more fully deployed, will very effectively deter aliens who are

counterfeiting documents and making fraudulent attempts at entry to the United States. We already see datashare undermining those who photo-substitute their visas or try to use someone else's document. Once inspectors at the ports of entry or our visa officers detect such cases, they can strongly support their findings with improved evidence supplied through Consular Affairs data such as digitized photos, the text of the visa issuance or refusal and longer comments accompanying Consular Affairs' lookout data.

Since ADNET/NCI (Anti-Drug Network/Nigerian Crime Initiative) is a compendium of law enforcement data, wouldn't this tool be useful in each visa unit overseas?

The Visa Office is familiar with ADNET and held discussions with the project leaders in January 1999. Overall the Department, with the Bureau of Diplomatic Security in the lead, has regularly participated in ADNET/NCI working group. Diplomatic Security has provided data in the form of case summaries to the ADNET/Nigerian Crime Initiative Database. This tool is particularly valuable to investigators and intelligence analysts addressing organized crime. (See appendix expanding on DS' participation in ADNET/NCI.)

The Visa Office would like to ensure that it has timely intelligence information concerning international

organized crime so that consular officers and other State Department employees can use such information to determine whether individuals applying for visas may be ineligible based on connections with international crime. Once the intelligence analysts can make hard findings or confirm any ineligibility for organized criminal activity, the Visa Office would like to have this data. Consular Affairs recommends our law enforcement colleagues immediately share this information with us in the form of lookout extracts we can place in the Consular Lookout and Support System. CLASS is our primary screening tool for over 9.5 million visa applications per year. It is tailored to our visa operations environment where we need to handle the data in an unclassified form. Our visa officers, who process a heavy workload, must perform namechecks within three to five seconds. The more interagency data in our namecheck system, the better we can do our job. We can protect sensitive lookout data with codes that stop visa issuance in certain cases and require visa officers to refer the cases to Consular Affairs for Security Advisory Opinions.

Mr. Chairman and Members of the Committee, we would be more than happy to discuss the matters I have raised or any others including interagency datashare and border security at your convenience. As I said at the outset Consular

Affairs is reliant on its modernized automation and interagency datashare to achieve its mission to facilitate legitimate travel and to protect our borders. In this overview I pointed to several successes, but we still have much work to complete in this area. Again, thank you for the opportunity to share with you our thoughts on this important topic. I will be happy to answer any questions you may have.

Addendum from Bureau of Diplomatic Security, US Department of State

July 12, 2001

INTERAGENCY DATASHARING - ADNET/NCI AND INTERPOL

With the exception of cases involving U.S. citizens, the data provided by the Bureau of Diplomatic Security to ADNET encompasses all of its criminal investigative cases. This information is available only to federal law enforcement entities participating in the ADNET communications and data sharing system. In the event a global ADNET data base search reveals a potential match with the subject of an inquiry, ADNET provides the investigating agency with the DS case summary and point of contact for further information. ADNET provides a means by which federal law enforcement groups can communicate and share criminal intelligence data directly in real time. Agencies participating in ADNET include DEA, FBI, INS, USCS, USMS, USPIS, and USSS. DS Special Agents assigned to CA's Fraud Prevention Unit in Lagos, Nigeria use ADNET/NCI as an investigative tool to screen for visa applicants who would otherwise be ineligible for U.S. visas.

Additionally, CA and DS have discussed with the INTERPOL U.S. National Central Bureau the sharing of INTERPOL's international criminal database with the Department for the purpose of avoiding issuance of U.S. visas to known international criminals. Unfortunately, USNCB has been unable to obtain the funds to facilitate electronic datasharing with CA, or with DS and other US law enforcement agencies.

Mr. SHAYS. Colonel Deacy.

Colonel DEACY. Thank you, Mr. Chairman, for this opportunity to testify before your subcommittee. I have submitted a written statement for the record, and I will proceed now with brief oral remarks.

Mr. SHAYS. Please move your mic a little closer.

Colonel DEACY. I am Colonel Mike Deacy, Assistant Deputy Director for Information Engineering at the Defense Information Systems Agency [DISA], Department of Defense.

The agency began in 1960 as a defense communications agency charged with consolidating the communications functions common to the military department at that time. In 1991, the name was changed to DISA, to reflect the agency's role in providing total information systems support to the Defense Department.

The DISA commander is dual-hatted as Director, DISA, and Manager of the National Communications System. National Communications System is a confederation of 23 Federal departments and agencies in cooperation with 30 private companies responsible for the availability of a viable national security and emergency preparedness telecommunications infrastructure.

The White House Communications Agency is also managed under DISA. The DISA Vice Director is dual-hatted as commander of the Joint Task Force Computer Network Operations.

DISA is a Department of Defense combat support agency under the direction, authority and control of the Assistant Secretary of Defense for Command, Control, Communications and Intelligence. DISA provides reliable, flexible, affordable and effective communications and information systems support to warfighters, regardless of their location, mission, or the military service or allied nation with which they are affiliated.

DISA plans, develops, supports command, control, communications, computer and intelligence and information systems that serve the needs of the national command authorities under all conditions during peace or war.

DISA ensures the interoperability and integration of C4I systems. The Global Command and Control System is the premier command and control system in support of national command authorities, warfighting commanders in chief and joint task force commanders.

The global combat support system interfaces, integrates and displays information from authoritative DOD-wide service and agency-sponsored combat support systems. The Defense Information System Network data networks include the unclassified but sensitive Internet Protocol Router network, or NIPRNet, and the Secret Internet Protocol Router network, SIPRNet. These two data networks provide the essential information necessary to conduct and support the full range of military operations.

The Defense Message System is the ASD C3I designated messaging system for DOD and supporting agencies. The Defense Information infrastructure common operating environment is the foundation infrastructure for building interoperable C2 systems.

In partnership with the Defense Logistics Agency, we provide engineering support for the Joint Electronic Commerce Program of-

fice. This effort will make electronic commerce electronic business a reality between DOD and its commercial partners.

We work closely with theatre and tactical command and control systems, allied C4 systems and those national and international commercial systems that affect DISA's mission.

DISA Western Hemisphere, or WESTHEM provides world class information products and services to DISA customers in the Western Hemisphere and global systems management of deployed portions of the Defense Information System network.

In partnership with the National Security Agency, we also provide engineering for the DOD public key infrastructure program.

One of our assigned projects is the Anti-Drug Network, ADNET. Our ADNET office is located within the information engineering organization, the smallest of its nine divisions.

DISA works two multi-agency projects for the law enforcement community as the technical agent for computers and communications. The first project, ADNET, serves the military, intelligence and law enforcement communities, sharing counter-drug information at the secret collateral level.

The second project supports the Nigerian Organized Crime Strategy of the Departments of Justice, State, Treasury and the U.S. Postal Service by assisting those organizations in the sharing of sensitive law enforcement information within a secret environment.

ADNET is a component of our response to congressional tasking in the 1989 Defense Authorization Act. By taking advantage of the existing military command and control network used across the Department, ADNET expanded to serve 17 key detection and monitoring locations by early 1990, and totaled over 30 sites by 1991.

There were a number of concerns cross the counter-drug community as this information sharing environment grew. We ensured that the Joint Staff validated each and every new site in the ADNET community of interest.

In 1994, the executive office of the President, Office of National Drug Control Policy [ONDCP], sponsored the National Interdiction Command and Control Plan [NICCP]. The NICCP directed that, "ADNET will be the primary communications interface for passing counter-drug command, control and tactically actionable information among the three intelligence centers." DISA supported this effort as it engineered upgrades to the overall networking environment.

In 1995, ONDCP and the drug intelligence community, which includes defense law enforcement and foreign intelligence agencies, developed and signed the Interdiction Intelligence Support Plan. The support plan designated ADNET as the principal tool for sharing counter-drug intelligence among the interdiction centers/components and supporting drug intelligence community.

The ISSP also tasked the ADNET program to initiate new forms of information sharing based on World Wide Web technology. DISA supported this effort and made possible quantities of data-sharing. Over 50 Federal entities are now members of the ADNET community and they operate from over 130 sites worldwide.

As for the second effort, from the Defense perspective, our support to the Nigerian Organized Crime Strategy is based on PDD–42, International Organized Crime, November 1995.

In 1997, senior Justice Department representatives requested an enhancement in the ADNET model for information sharing to include hosting sensitive law enforcement data with access from nine Federal agencies.

The agencies had no way to interconnect themselves across any other common network. As a Federal agency tasked to support PDD–42, DISA made it clear that while this could not be funded by Defense appropriations, DISA could support an innovative information sharing effort with funding by the participating agencies.

Funding began in 1998, and DISA developed a distributed data base environment with query capability across the agencies, along with security controls.

Once again, I thank you for the opportunity to appear before the subcommittee. I will answer any questions you have to the best of my ability and take questions for the record that are beyond my capability to respond to at this time.

[The prepared statement of Colonel Deacy follows:]

TESTIMONY OF THE ASSISTANT DEPUTY DIRECTOR

FOR INFORMATION ENGINEERING,

DEFENSE INFORMATION SYSTEMS AGENCY,

BEFORE THE

HOUSE COMMITTEE ON GOVERNMENT REFORM,

SUBCOMMITTEE ON NATIONAL SECURITY,

VETERANS AFFAIRS, AND INTERNATIONAL RELATIONS

CLEARED
FOR OPEN PUBLICATION
JUL 18 2001
DIRECTORATE FOR FREEDOM OF INFORMATION
AND SECURITY REVIEW
DEPARTMENT OF DEFENSE

JULY 24, 2001

Thank you, Mr. Chairman, for this opportunity to testify before your subcommittee. I am Colonel Michael Deacy, Assistant Deputy Director for Information Engineering at the Defense Information Systems Agency (DISA), Department of Defense (DoD). The Agency began in 1960 as the Defense Communications Agency (DCA) charged with consolidating the communications functions common to the military departments at that time. In 1991, the name was changed to DISA to reflect the Agency's role in providing total information systems support to the Defense Department. The DISA Commander is dual-hatted as Director, DISA, and Manager, National Communications System (NCS). The White House Communications Agency (WHCA) is also managed under DISA auspices.

01-C-00709

DISA is a Department of Defense (DoD) combat support agency under the direction, authority and control of the Assistant Secretary of Defense for Command, Control, Communications and Intelligence (ASD {C3I}). DISA provides reliable, flexible, affordable, and effective communications and information systems support to warfighters regardless of their location, mission, or what military service or allied nation with which they are affiliated. DISA plans, develops, and supports command, control, communications, computers and intelligence (C41) and information systems that serve the needs of the National Command Authorities (NCA) under all conditions during peace or war. It provides guidance and support on technical and operational C3 and information systems issues and coordinates DoD planning and policy for the integration of C4I systems and the insertion of C4I for the Warrior (C4IFTW) leading edge technologies into the Global Information Grid (GIG).

NCS is a confederation of 23 Federal Departments and Agencies, in cooperation with 30 private companies, tasked with ensuring the availability of a viable national security and emergency preparedness telecommunications infrastructure. Availability must be assured under all circumstances, including crisis or emergency, attack,

recovery and reconstitution. NCS assists the President, the National Security Council (NSC), the Office of Science and Technology Policy (OSTP), and the Office of Management and Budget (OMB) in the exercise of the telecommunications functions and responsibilities.

WHCA provides telecommunications and related support to the President, Vice President, White House Senior Staff, National Security Council, U.S. Secret Service and others as directed by the White House Military Office. This support includes non-secure voice, secure voice, record communications, automated data processing support and other services both in Washington, D.C. and at trip sites worldwide.

The DISA mission is warfighter support at all levels, within all situations, around the globe. DISA provides a seamless web of communications networks, computers, software, databases, applications and other capabilities that meet the information processing and transport needs of DoD. DISA is committed to Information Assurance (IA) through its innovative IA initiatives. The Agency ensures the interoperability and integration of C4I systems such as the Global Command and Control System (GCCS), Global Combat Support System (GCSS), Defense Information System Network

(DISN), and Defense Message System (DMS). We provide the foundation infrastructure for building interoperable C2 systems through the Defense Information Infrastructure Common Operating Environment (DII COE). DISA also partners with the Defense Logistics Agency (DLA) to make electronic commerce/electronic business (EC/EB) a reality between the DoD and its commercial partners. We work closely with theater and tactical command and control systems, Allied C4 systems, and those national and international commercial systems that affect DISA's mission. DISA Western Hemisphere (WESTHEM) provides world-class information products and services to DISA customers in the Western Hemisphere and global systems management of deployed portions of the Defense Information System Network (DISN).

DISA has a strong commitment to protect DoD computer networks from cyber attacks. The DISA Vice Director is the Commander of the Joint Task Force Computer Network Operations (JTF-CNO). JTF-CNO was assigned to CINCSPACE in October 1999. CINCSPACE elected to keep the Task Force collocated with DISA's Global Network Operations and Security Center (GNOSC) and the DoD Computer Emergency Response Team (DoD-CERT). Our people monitor networks for malicious activity, analyze activity, take corrective action whenever possible, and report incidents. Incident

reports provide critical technical information that is fused with details concerning ongoing operational missions, as well as with information from embedded intelligence, counter-intelligence, and law enforcement channels. This quick-response, systematic, and repeatable process is essential to developing operational impact assessments, identifying responsive courses of action, and coordinating necessary actions with appropriate organizations.

In addition to responding to current and future network cyber attacks, DISA has a strong infrastructure IA program. DISA provides the engineering for the DoD Public Key Infrastructure (PKI) program. On the NIPRNet and SIPRNnet networks, PKI provides authentication of sender, data integrity, data confidentiality, recipient authentication, non-repudiation of transmission/transaction, and access control to networks and web servers. PKI is integrated with work supporting Global Directory Services (GDS). GDS will implement a joint interoperable directory service to give warfighters the ability to locate people, resources, and applications at any time or place. It will also serve as a repository for policy, authentication, and access control attributes.

Six of our premier programs demonstrate the breadth and sccpe of the DISA mission. These programs, GCCS, GCSS, DISN, DMS, DII COE, and EC/EB are representative of our C3I, Global Information Grid (GIG) foundation, and business support. Our WESTHEM Commander, managing the five Defense Enterprise Computing Centers (DECC), ensures state-of-the-art transaction processing to DoD customers.

The Global Command and Control System (GCCS) is the premier command and control (C2) system in support of the National Command Authories (NCA), warfighting Commanders-In-Chief (CINCs), and Joint Task Force (JTF) Commanders. It is part of the Chairman of the Joint Chiefs of Staff vision for providing high quality and timely support to the joint warfighter. GCCS supports forces for joint and combined operations throughout the spectrum of conflict anytime and anywhere in the world with compatible, interoperable, mobile, deployable, and integrated C4I systems. The GCCS Common Operational Picture (COP) correlates and fuses data from multiple sensors and intelligence sources to provide warfighters the situational awareness needed to act and react defensively.

The Global Combat Support System (GCSS) is a demand driven, joint warfighter focused initiative to accelerate delivery

of improved combat support capabilities. It interfaces, integrates, and displays information from authoritative DoD-wide Service and Agency sponsored combat support systems. The GCSS delivers the potential for focused logistics by providing a fused and integrated combat support picture of the battlespace to the warfighter as a whole. Through GCSS, the joint warfighter has a single, end-to-end capability to manage and monitor units, personnel, and equipment from mobilization through deployment, employment, sustainment, redeployment, and demobilization

The Defense Information System Network (DISN) is the DoD's consolidated worldwide enterprise-level telecommunications infrastructure that provides the end-to-end information transfer network for supporting military operations. It is transparent to its users, facilitates the management of information resources, and is responsive to national security and defense needs under all conditions in the most efficient manner. DISN is an end-to-end infrastructure comprised of three major segments or blocks consisting of the sustaining base, long haul, and deployed assets. The DISN data networks include the Unclassified But Sensitive Internet Protocol Router Network, or "NIPRNet" and the Secret Internet Protocol Router Network, or "SIPRNet." The

essentiality of these networks has developed over time, and has been accelerated by the increasing dependence of the DoD on the Internet as a common business process infrastructure. Taken together, these two data networks provide the essential information necessary to conduct and support the full range of military operations, and support our warfighters, the Office of the Secretary of Defense, the Joint Chiefs of Staff, the Commanders-in-Chief, the Military Services, the Defense Agencies, and other Federal Agencies. In addition, these networks will continue to grow in importance to the Department of Defense as "Community of Interest" networks are developed and fielded. These Service-specific networks will be using the NIPRNet and SIPRNet as the common data transport infrastructure.

The Defense Message System (DMS) is the ASD C3I designated messaging system for DoD and supporting agencies. When fully deployed, DMS will provide organizational and individual message service to all DoD users (to include deployed tactical users), access to and from DoD locations worldwide, and interfaces to other U.S. government agencies, allies, and Defense contractors. DMS will reliably handle information of all classification levels (Unclassified to Top Secret), compartments, and handling instructions. DMS relies on both existing and emerging

technologies to meet the Department of Defense's (DoD's) need for secure, accountable, organization-to-organization and individual messaging at reduced cost. DMS will provide the approved minimum essential secure messaging and directory services to support the closure of the Automatic Digital Network (AUTODIN).

The Defense Information Infrastructure Common Operating Environment (DII COE) establishes an integrated software infrastructure, which facilitates the migration and implementation of functional mission applications and integrated databases across systems. It provides software components, architecture principles, guidelines, and methodologies that assist in the development of interoperable mission application software by capitalizing on a thorough, cohesive set of infrastructure support services. The DII COE is either used in or planned for use in 130 C2 systems.

The Electronic Commerce/Electronic business (EC/EB) partnership with the Defense Logistics Agency (DLA), established in 1998 through the creation of the Joint Electronic Commerce Program Office (JECPO), develops applications to present a single face to industry while providing all Services and Agencies with a secure,

standards-based infrastructure to handle day-to-day business.

DISA WESTHEM provides policy and guidance for the operation of WESTHEM field activities located throughout the continental U.S. These facilities are highly automated data processing nodes responsible for the DOD's personnel, payroll, logistics, accounting and medical records processing. In addition, WESTHEM provides central C2 for its field activities and world class, secure, data processing facilities for both mainframe and mid-tier environments. DISA WESTHEM serves globally as the single system manager for deployed components of the Defense Information Systems Network (DISN). The DECCs provide quality Information Technology (IT) systems services in support of the nation's warfighter customer requirements through integrated management of research, development, acquisition and support for sustainment of superior IT systems.

One of our assigned projects is Anti-Drug Network (ADNET). Our ADNET office is located within the Information Engineering organization and is the smallest of its nine divisions. DISA works two multi-agency projects for the law enforcement community wherein we serve as the technical

agents for computers and communications. The first project, ADNET, serves the military, intelligence, and law enforcement communities sharing counter-drug information at the SECRET collateral level. The second project supports the Nigerian Organized Crime Strategy of the Departments of Justice, State, Treasury, and the US Postal Service by assisting those organizations in the sharing of sensitive law enforcement information within the SECRET environment.

ADNET is a component of our response to Congressional tasking in the 1989 Defense Authorization Act.

By taking advantage of the existing military command and control network used across the Department (DSNET1), ADNET expanded to serve 17 key detection and monitoring locations by early 1990 and totaled over 30 sites by 1991. These sites included Joint Task Forces headed by DoD and the US Coast Guard, US Customs Service intelligence and air operations, Drug Enforcement Administration, Federal Bureau of Investigation, law enforcement intelligence centers, the Intelligence Community, and others.

There were a number of concerns across the counter drug community as this information-sharing environment grew, including some organizations within the Defense Department.

We ensured that the Joint Staff validated each and every new site in the ADNET community of interest. As the effort evolved, we required accreditation according to Defense standards of each and every site. We instituted remote security auditing of sites using sophisticated new technologies. We also instituted limitations on access to law enforcement information by Defense personnel.

In 1994, the Executive Office of the President, Office of National Drug Control Policy (ONDCP), sponsored the National Interdiction Command and Control Plan (NICCP). Signed by the Deputy Assistant Secretary of Defense for Drug Enforcement Policy and Support (DEP&S), the Commandant of the Coast Guard, the Commissioner of U.S. Customs, and the Director of ONDCP, the NICCP directed that "ADNET will be the primary communications interface for passing counter drug command, control, and tactically actionable information among the three [intelligence] centers." DISA supported this effort as it engineered upgrades to the overall networking environment.

In 1995, ONDCP and the "drug intelligence community" (including Defense law enforcement and foreign intelligence agencies) developed and signed the Interdiction Intelligence Support Plan (IISP). The IISP designated

ADNET as the principal tool for sharing counterdrug intelligence among the interdiction centers/components and supporting drug intelligence community. The ISSP also tasked the ADNET program to initiate new forms of information sharing based on World Wide Web technology. DISA supported this effort and made possible quantities of data sharing. Over 50 Federal entities now are members of the ADNET community and they operate from over 130 sites worldwide.

As for the second effort, from the Defense perspective, our support to the Nigerian Organized Crime Strategy is based on Presidential Decision Directive 42 (PDD-42), International Organized Crime, November 1995.

Senior Justice Department representatives requested in 1997 an enhancement in the ADNET model for information sharing to include hosting sensitive law enforcement data with access from 9 Federal agencies. The agencies had no way to interconnect themselves across any other common network.

As a Federal agency tasked to support PDD-42, we made it clear that while this could not be funded by Defense appropriations, DISA could support an innovative information sharing effort with funding by the

participating agencies. Funding began in 1998 and we developed a distributed database environment with query capability across the agencies along with security controls. Today there are more than 1.5 million records among the 15 law enforcement databases and the participants make thousands of queries each month.

Once again, I thank you for the opportunity to appear before this subcommittee. I will answer any questions you may have to the best of my ability and take questions for the record that are beyond my capability to respond on the spot today.

Mr. SHAYS. Thank you very much.

Let me confess that when we talk about information systems, sometimes my eyelids start to go down a little bit, and I notice some of the people in audience, they start to—their heads start to droop.

But I consider this a very, very important issue. And the logic that I take to this is, of course, we would want to share this information, subject to wanting to make sure that civil liberties aren't, you know, compromised and that data isn't compromised.

Colonel Deacy, you said basically we had 13 sites, to go to 30. I just want to be clear. That is the only—first off, how many sites are there? You told—now my understanding, Colonel, is there are only a few places that you can access information, correct?

Colonel DEACY. No, sir. There are actually many places.

Mr. SHAYS. OK. Then I misunderstand the concept in your document when—maybe that is when my eyes started to droop too low, my eyelids. What was the mention of sites? We talked about sites, and they——

Colonel DEACY. Yes, sir. That is where I mentioned the initial starting number of sites.

Mr. SHAYS. OK. You are going to have to talk a little bit louder. Hit that mic, just—I just dislike these mics, I guess.

Colonel DEACY. Sir, the key is that there are 50 Federal entities that can access this data, which belong to us.

Mr. SHAYS. Anywhere? The term—or are there only certain places where they can get this information?

Colonel DEACY. There are only certain places.

Mr. SHAYS. That is what my question was. How many places are there presently?

Colonel DEACY. Sir, for a specific number, I will have to take that for the record. But, I believe it's in the range of 130 locations.

But let me take that for the record for a specific answer.

Mr. SHAYS. All right. Well, when I am asking, the gentleman behind you was nodding his head. So maybe he would be able to——

Colonel DEACY. That is specific, 130.

Mr. SHAYS. OK. And only in those sites can you access the information, correct?

Colonel DEACY. That is the way the system is configured and our security controls tend to ensure that. There is no 100 percent security.

Mr. SHAYS. My understanding is—I mean, I—when we started this hearing, I saw, Anti-Drug Network/Nigeria Crime Initiative. The reason why we took Nigeria as a pilot program is that Nigeria seemed to interface the—their activities interfaced a whole host of different agencies.

Right, Mr. Swartz?

Mr. SWARTZ. Yes, sir. That is certainly one of the reasons. It seemed like a logical pilot project simply because there were a number of different law enforcement agencies that dealt with one aspect or another of the problem.

Mr. SHAYS. I am unclear as to whether this was administrative driven or legislatively driven, this effort.

Mr. SWARTZ. The ADNET itself, as I understand it, Mr. Chairman, was legislatively driven. And then there were administrative followups that made ADNET into the Anti-Drug Network.

The Nigerian Organized Crime Initiative, my understanding, was driven largely in response to PDD–42 and in response to the escalation of Nigerian organized crime, building upon work that had already been done by law enforcement agencies, including through interagency task——

Mr. SHAYS. Should I make an assumption that basically this was not something that really came from the Department? I mean, right now, candidly—and this is not to beat up on anybody, but this program is stalled.

It is not—and my wife works for the Peace Corps and she has an important position there. But we don't have a Director of the Peace Corps, and certain things aren't happening at the Peace Corps until you get a Director.

Is some of what we are seeing here the result of just key people not being there?

What—how should I interpret this with—first off, do you agree that we are not moving ahead, full speed ahead?

Mr. SWARTZ. Speaking for the Department of Justice, I think it is fair to say that the transition from one administration to the next has led to the need to reassess how we go forward with this initiative.

In terms of being stalled, I think it is still the case that the Nigerian Organized Crime Initiative on ADNET continues to be used. As I mentioned in my testimony, there are approximately 1,000 hits per month that are—that are now—queries being made on the network.

Mr. SHAYS. But that system is only as good as what comes into it.

Mr. SWARTZ. That's correct.

Mr. SHAYS. You know, I get the sense—I was thinking that maybe we should have had the FBI and the DEA here too, but Justice—and the INS here. But basically Justice has decided to speak through you on this issue.

And, I—we don't have the sense that there is the kind of cooperation from some of these departments as there—agencies as we would like.

Mr. SWARTZ. I would say, from the Department of Justice's perspective, the primary issue now confronting the Department is the uploading of full text reports, 302s in the case of FBI and otherwise, and how that should go forward, what the utility of that is.

That is one thing that the Department does want to study, largely because the resources that are—need to be devoted to that are extensive. As the basic policy establishing ADNET makes clear—excuse me, the Nigerian Crime Initiative on ADNET makes clear, there are a number of items that have to be vetted in each report before it can be uploaded to ADNET. That does take a significant amount of time and resources.

But I do want to make clear that the Department is not wavering in its desire to fight Nigerian organized crime. The question is only what is the most effective use of our resources and should

ADNET be moving more toward an indexing system for this system——

Mr. SHAYS. And you are talking about Nigerian crime. I am thinking of this as a system that was a pilot program to demonstrate that we could do what logically seems to me to be appropriate; and that is, to have different law enforcement agencies share information, which they are very reluctant to do.

Let me just get in with some of these questions in some sense of order.

To what extent are the member agencies fully committed to funding participating and sharing data with ADNET/NCI? And I would like to ask you that question, Mr. Swartz. I mean, to what extent are they fully committed?

Mr. SWARTZ. I think it is fair to say within the Department of Justice now, the various law enforcement agencies, there is not unanimity as to the utility of funding ADNET, the ADNET portion of the Nigerian Crime Initiative at its current levels.

Again, it is a question of each agency trying to balance its resources, not——

Mr. SHAYS. But they have the ability not to fund it if they don't want to?

Mr. SWARTZ. That is a question that the administration is considering, whether each agency—how it should be required to go forward with regard to funding this.

Mr. SHAYS. Why do FBI and DEA have zero inquiries into ADNET and NCI for over the last few months? They had practically no inquiries.

Mr. SWARTZ. I believe, Mr. Chairman—I can go back and determine this directly from the DEA and FBI, but my understanding is, it is a result of whether or not their particular investigations led them to make use of the data base for any such queries.

Mr. SHAYS. Say that last thing again, please.

Mr. SWARTZ. It would be a question of whether or not the investigations they are conducting led them to make inquiries on the data base.

Mr. SHAYS. Or is it that they just simply don't think there is information in there that would be helpful, or is it that they think that they have the information, which they are not sharing? If they are not making inquiries, are they also providing data to this system?

Mr. SWARTZ. Well, the FBI has, in fact, uploaded full text records in many cases.

Mr. SHAYS. On a timely basis?

Mr. SWARTZ. They have been doing it on a timely basis. I think the question is what to do on a going-forward basis, whether they should be going to a pointer index system rather than loading full text records. But I think their record in the past of loading such records has been one of going forward.

Mr. SHAYS. So what agencies are participating fully and what agencies aren't, with the Nigerian Crime Task Force locations?

Mr. SWARTZ. In the task force locations?

Mr. SHAYS. Yes.

Mr. SWARTZ. Perhaps Secret Service could address that.

Mr. TOWNSEND. Mr. Chairman, I can go site by site if you would like the participants.

The New York field office, there are 22 full-time Secret Service special agents, two from the Postal Inspection Service, one from the FBI, one from the DEA, one from the INS and one from the Social Security Administration, OIG. Those are the full-time participants.

Would you like me to continue?

Mr. SHAYS. Who is left out?

Mr. TOWNSEND. The Department of State participates on an ad hoc basis, which is allowed by the MOU.

And additionally there are full-time local police officers; of course, we are speaking of the Nigerian Crime Initiative. Due to security clearance issues, their access to ADNET is limited. In New York, it is three from the NYPD.

I have that additional information which I can submit for the record or give it to you now.

Mr. SHAYS. So who, in your mind, is left out?

Mr. TOWNSEND. Well, in the case of New York, that is a pretty comprehensive view of Federal law enforcement. I think I named pretty much all of the major players there.

Mr. SHAYS. OK.

What is DOJ's program plan for expanding ADNET terminal installations, domestically and overseas?

Mr. SWARTZ. The expansion of the Nigerian Organized Crime Initiative/ADNET site is one that is established not simply by DOJ, but it is part of the MOU. The memorandum of understanding called for 12 task force sites, five headquarters sites and one site abroad. In fact, my understanding is that we have had eight sites installed, to date, according to DISA, and eight headquarters sites. And abroad as I mentioned, one in Nigeria, one in Ghana.

Mr. SHAYS. Let me just conclude, Mr. Swartz, with this first round, then go to Mr. Gilman.

You are here, but the FBI and the DEA aren't here. I am just curious to know why there is not participation on their part. I would think they would be wanting to participate more than anyone else.

Is it that they feel that the information that they can get, they already have; that they are basically the in-puters and not that they don't see much plus in utilizing this information?

Mr. SWARTZ. I do want to make clear that the FBI and the DEA have participated in the past, both financially and in records being supplied to the system.

I do think that the usefulness of this system to each agency will depend in part, as you suggested, on whether the agency believes that it has the records that it already needs for the particular aspect of the Nigerian organized crime that it is dealing with.

But again, as Mr. Townsend has suggested, the FBI, and in some cases, the DEA do participate in task force activities and are participating through other means as well.

Mr. SHAYS. Is this a good program, Mr. Swartz?

Mr. SWARTZ. Again, I think it is important to distinguish between the two programs. I think that the Nigerian Organized Crime Initiative, that is the idea of task force, is essential. I think that all Federal agencies would agree that we need to engage in

information sharing; similarly, I think that the idea of ADNET, of information sharing as you suggest, is a very important one.

And this system is a powerful one. I think the issue that we face, that critical issue that I have seen with regard to this, is how you effectively make access available to the preexisting data bases in each Federal law enforcement agency and whether, because of constraints required by Rule 6E, grand jury materials or privacy——

Mr. SHAYS. Privacy and what was the other one?

Mr. SWARTZ. Rule 6E, the grand jury secrecy issue, the Privacy Act, questions that may go to confidentiality of informants, whether it is necessary, as has happened with this initiative, for each record to be vetted, if you will, to be cleared before it is put into a separate data base that can be accessed to the initiative. That is a time-consuming and expensive operation, one that I think that the administration has to consider as to whether it is the most effective way to share information or whether, alternatively, we might think of, for instance, an index system.

But, again, this may be something that the Secret Service——

Mr. SHAYS. Let me just ask one last question. I am sorry, but is this system totally and completely secure, or are there concerns that it can be compromised; and who would be prepared to answer that?

Colonel DEACY. Sir, security is something of a risk management endeavor. We endeavor for 100 percent security, but you are never sure of what the enemy's—for example——

Mr. SHAYS. If someone on the outside were to look at this system, would they say this is an easy system to penetrate?

Colonel DEACY. No, sir.

Mr. SHAYS. OK. Even though we have terminals so many different places.

Colonel DEACY. That is correct. They would not say it is an easy system to penetrate.

Mr. SHAYS. OK.

Mr. Gilman, would you like the floor?

Mr. GILMAN. Thank you, Mr. Chairman. I want to thank you for conducting this hearing. The state of the Federal interagency data-sharing program is important to all of us, and as a former chairman of our International Relations Committee, I was in complete agreement with President Clinton's decision declaring international crime a threat to our national security, and threats posed from transnational criminal organizations, including the Nigerian heroin traffickers, South American drug cartels, Russian organized crime and Asian triads were and still are great threats to our Nation.

Accordingly, I applauded the President's decision to increase interagency cooperation against both these organizations and those engaged in money laundering.

In the 5 years since the issuance of the Clinton Executive order, the process of fostering greater interagency information, interagency communication has been with mixed results while some progress has been made with the creation of an Anti-Drug Network, ADNET, data base to share interagency information, these efforts have not realized their full potential, and greater interagency cooperation has been impeded by traditional jurisdictional turf battles, legal challenges, including privacy, the civil rights

issues, bureaucratic inertia, high turnover rates among personnel and funding problems from the participating agencies.

Despite these ongoing problems, the challenges posed by transnational criminal organizations remain. If anything, these entities are as dangerous today, if not more so, than they were back in 1996 when that Executive order was issued.

It is gratifying, Mr. Chairman, that this subcommittee has had the opportunity to bring some experts in on the front lines in order to review the status of interagency data-sharing and our progress in interagency cooperation can be improved.

Let me ask our panelists. Do you see the need for some central authority right now to review how more effectively we can have interagency sharing of information?

Mr. Swartz.

Mr. SWARTZ. Thank you, Mr. Gilman.

Certainly the Department of Justice believes that it is necessary internally to assess the various means of interagency sharing, of which ADNET, of course, is one both with regard to its Nigerian crime aspect and more broadly as we use it for other aspects, including the anti-drug aspect.

But we have, of course, in the context of the drug interdiction work, have been building the strategy for interagency sharing, and that is certainly one area that we believe that the Department should assess on an ongoing——

Mr. GILMAN. Well, have you been using that? Beyond Nigeria has that been utilized?

Mr. SWARTZ. Yes, ADNET does have the capacity and is used for secure communications in other contexts for law enforcement purposes, and began, in its essence, as an anti-drug network.

Mr. GILMAN. Do you supply information to DEA, for example?

Mr. SWARTZ. Well, through ADNET—and again DISA can correct me, but my understanding is that ADNET can be used to access other preexisting law enforcement data bases such as EPIC if there is, in fact, a clearance for the particular user. So it is in essence, ADNET is basically a framework through which law enforcement data bases can be accessed. In that regard, it's an extremely powerful device for law enforcement.

Mr. GILMAN. So all Federal law enforcement agencies can make use of ADNET?

Mr. SWARTZ. If they have the proper clearance and proper interconnections. And, again, some law enforcement agencies are moving to make sure that they do have access to ADNET.

Mr. GILMAN. Well, are there some that do not have that kind of proper equipment?

Mr. SWARTZ. My understanding is that the—and, again, I can be corrected—that the headquarters operations of Federal law enforcement agencies all do have ADNET access and that a number of field offices of different law enforcement agencies have ADNET access as well.

Mr. GILMAN. Are there some that do not? Is there something that your agency can do to help them acquire that ability?

Mr. SWARTZ. I would have to take that question, and I'll answer it for the record.

Mr. GILMAN. Mr. Townsend, my question about whether there should be some sort of central oversight.

Mr. TOWNSEND. Thank you, Mr. Gilman.

Two things strike me here. We are talking about two separate but related issues, the ADNET system and its use in the Nigerian Crime Initiative itself——

Mr. GILMAN. Let's not just concentrate on Nigeria. But what about for all the law enforcement people?

Mr. TOWNSEND. Well, clearly information sharing is where we have to get stronger in law enforcement and——

Mr. GILMAN. Well, then should there be some central oversight agency to do that?

Mr. TOWNSEND. Sir, my response to that would be, we in the Secret Service would look for commitment at the departmental level for law enforcement agencies' participation to be mandated in this program, if that were the desire of that department.

Mr. GILMAN. Well, here we have an Executive order going back to 1996 by President Clinton asking that this be done, and apparently it hasn't been fully carried out. What do you think is needed to do that?

Mr. TOWNSEND. I would say that commitment at the departmental level for the agencies residing within that department.

Mr. GILMAN. And that's not there at the present time, that kind of commitment isn't?

Mr. TOWNSEND. It depends on the location around the country operationally. At the headquarters level, we share information well, and the field tends to share it well also. But the various departments, because of their mandates, their different mandates—Justice having a very wide mandate, Treasury having a much narrower mandate—have competing——

Mr. GILMAN. Ms. Barry.

Ms. BARRY. Yes, sir. Well, from the perspective of a consular officer overseas, we are working in an unclassified environment, and so we are really looking for tools like ADNET to have direct access to the records of law enforcement agencies. Our CLASS Lookout System points the way to the agency that owns the information.

Mr. GILMAN. Well, don't you with consular activity have to approve visas? Didn't we revise the system for you so that you could have information on the background of anyone applying for a visa that had a criminal record?

Ms. BARRY. Yes, sir. And as we have detailed, I think, in our written statement for the record, we receive routinely many records from other foreign—from the law enforcement agencies.

Mr. GILMAN. Well, wouldn't that be of help to you in that direction?

Ms. BARRY. It is of immense help. What happens is that when we get a hit, the headquarters here goes back to the owner of that information and provides that information, or the gist of it, to the consular officer in the field. Or, if we don't have a hard finding yet, we simply have information that points to a problem of concern, we point out to the consular officer lines of questioning to pursue or the types of evidence that would help us reach a final determination.

Mr. GILMAN. Well, is your system working now out in the field where someone applying for a visa, do you automatically have information on whether or not he has a criminal record?

Ms. BARRY. Yes, we do, sir. In most instances, the one issue that we haven't really finalized yet is a better information system—data-share system with the FBI for which legislation is required.

Mr. GILMAN. What is holding up that kind of a sharing of information?

Ms. BARRY. Well——

Mr. GILMAN. You don't have any criminal record from the FBI then; is that right? Is that——

Ms. BARRY. We don't get it on the most timely basis, sir.

Mr. GILMAN. Well, what is—how timely do you get it?

You have a person applying for a visa. How long does it take you to find out whether he has a criminal record or not?

Ms. BARRY. Well, when we query the CLASS data base, it takes a matter of seconds to find out if there's a hit in the system. The NCIC data base is the one data base that we do not have connectivity to in the kind of real-time basis that we would like.

Mr. GILMAN. What would you like? How long does it take you to find out from the FBI whether this person has a criminal record? How long does it take you at the present time to find out whether he has a criminal record with the FBI?

Ms. BARRY. Just a minute.

Sir, if I can distinguish in my answer between immigrant visas and nonimmigrant visas. When we are adjudicating an immigrant visa application, we have access to the NCIC data base. We have an FBI agent who is part of our staff at the National Visa Center who accesses the NCIC data base on our behalf and gives us information on a timely basis so that the adjudication of an immigrant visa application is done in a timely manner——

Mr. GILMAN. Let me give you a hypothetical. Assume you have a terrorist getting a nonimmigrant visa from you. How would you find out whether or not he has a criminal record?

Ms. BARRY. For terrorism, there is a very specific program called TIPOFF. Analysts in the Department of State and the Bureau of Intelligence and Research feed our data base regularly, and so when we get a hit in that data base for someone suspected of terrorist activity, we go back to the INR Bureau to help us determine the full information.

Mr. GILMAN. So you have sufficient information now to determine whether a terrorist could be given a nonimmigrant visa?

Ms. BARRY. Yes, sir. It's a very active program.

Mr. GILMAN. What——

Ms. BARRY. I can tell you, if I may, that——

Mr. GILMAN. Do you have any need for improving the information that you're getting? Is there a need for your getting more information for your visa people?

Ms. BARRY. We have two objectives to improve our Datashare, and that's to improve our access to FBI records and to improve our access to Customs data on serious violators.

Mr. GILMAN. What do you need to improve that?

Ms. BARRY. Well, with Customs, we believe we can work that arrangement out directly between the two agencies——

Mr. GILMAN. What about the FBI?

Ms. BARRY. With FBI, we understand legal opinion is that we require a legislative fix.

Mr. GILMAN. Have you made a recommendation with regard to that?

Ms. BARRY. Yes, we have, sir.

Mr. GILMAN. Who did you make that recommendation to?

Ms. BARRY. I'm sorry, sir. We have to take the question for details. We have submitted some legislative ideas.

Mr. GILMAN. Will you let our committee know of any legislation that's needed?

Ms. BARRY. We will certainly do that.

Mr. GILMAN. And will you inform the chairman of that?

Ms. BARRY. I will be happy to, sir.

Mr. GILMAN. Thank you.

Colonel Deacy—is it Deacy, sir?

Colonel DEACY. Yes, sir. I'm here representing DISA. DISA's role is to implement solutions to satisfy the valid requirements of the users. So on all policy questions, I defer to the Justice Department.

Mr. GILMAN. So you have no——

Colonel DEACY. We have no position on that, sir.

Mr. GILMAN. Thank you.

Just one other question.

Mr. SHAYS. You always do this to me. You wait 'til the red light, and then you say, one more——

Mr. GILMAN. I'm sorry. All right. Go ahead, Mr. Chairman.

Mr. SHAYS. No. You have one other——

Mr. GILMAN. All right. What are the Department of Justice's plans, Mr. Swartz, expanding your ADNET program beyond Nigerian crime, and such areas as Russian organized crime or Asian gangs? Do you have any proposal to expand it?

Mr. SWARTZ. Mr. Gilman, that is one of the matters that is under consideration by the new administration, whether this pilot project has suggested the expansion to other areas——

Mr. GILMAN. What is your personal opinion? Should it be expanded?

Mr. SWARTZ. My personal opinion, Mr. Gilman, is that the system needs to be considered in several different possibilities, one of which is an indexing system as opposed to a full data retrieval system, that is, a full record, simply because indexing is less onerous in terms of the time for scanning the records, for vetting them to make sure that materials can't be loaded into the——

Mr. GILMAN. But this system can be beneficial to all crime enforcement people, right?

Mr. SWARTZ. There is certainly no doubt—and I do want to make clear that the Department of Justice strongly does favor interagency sharing of information with regard to fighting criminal——

Mr. GILMAN. I think we all favor that, but how are we accomplishing it?

Mr. SWARTZ. And the ADNET system has, we believe, great promise, but there are issues, including the issues of how are data bases created in each agency for ADNET, and, I should add, issues of access, because ADNET and ADNET terminals are not present at every agent's desk——

Mr. GILMAN. Well, I would like to make one request. If there is something that this committee can do to assist in expanding that program, please let us know.

Mr. SWARTZ. Thank you.

Mr. GILMAN. Thank you, Mr. Chairman.

Mr. SHAYS. I thank the gentleman. I appreciate his very helpful questions.

Mr. Otter.

Mr. OTTER. Thank you, Mr. Chairman, and my apologies to you and the panel for my tardiness this morning. If I'm going over some of the same ground that's already been plowed, I apologize for that as well.

But, Mr. Swartz, most of the questions relative to success or failure here have been directed at you, and so with your permission, I'm going to continue with that same direction.

Totally how many agencies are involved here?

Mr. SWARTZ. I believe that the answer to that, Mr. Otter, is that the agencies that load on—let me find my record here. There are 8 agencies and 15 data bases from those agencies involved in providing materials for the Nigerian Crime Initiative on ADNET.

Mr. OTTER. We didn't come up with a specific contribution from each agency for the overall funding of this, but I did see that there were funds committed. What has been the total commitment of funds for setting up this project?

Mr. SWARTZ. Approximately $7.5 million for——

Mr. OTTER. And is that in some way quoted back to each agency, or does everybody put up a certain amount of money—the same amount of money?

Mr. SWARTZ. No. It's been assessed to each agency——

Mr. SHAYS. Excuse me, Mr. Swartz. I'm really curious. What are you looking through?

Mr. SWARTZ. These materials are NCI—excuse me, Nigerian organized crime metrics material to——

Mr. SHAYS. I'm sorry to interrupt, but this is getting a little frustrating for me. This committee asked for a briefing and a hearing. Why were we only allowed the opportunity to have a hearing and not a briefing as well?

Mr. SWARTZ. Mr. Chairman, I can't respond to that issue. The materials here are DISA materials that I'm looking at.

Mr. SHAYS. So it's available to the committee, right?

Mr. SWARTZ. Certainly, as far as I'm aware.

Mr. SHAYS. OK. So I'd like that document.

Mr. SWARTZ. Certainly.

Mr. SHAYS. I mean, it's—what's—and no disrespect to any of the witnesses here, but we're kind of an eclectic group here. We don't have FBI. We don't have the DEA. The Justice is coming and speaking for these other agencies. I don't know why there was a reluctance to allow them to come testify. We have had more trouble putting together this hearing than we've had on most hearings, which to me illustrates—some people didn't want to come. They didn't want to talk about it. Other people wanted to come because they didn't want other people to come. And it's just—to me, it just points out what a mess this program is, quite candidly.

It may be that there just is uncertainty as to where they go, so we're trying to be careful what we say. But you're looking at basically charts and figures that should have been provided to the committee, it seems to me, and to my knowledge they weren't. And it just—it makes for, one, a boring hearing. It makes for an uninformed hearing. We don't get the opportunity to really get at the nub of this. I still feel like we're wandering around trying to get a handle on this program. You may know about the program, but we don't. We don't know how well it is working, and, boy, I'll tell you, by the time we're done, we won't know much more. And I am sorry to say that, but that's the feeling I get, and we're all probably answering to higher-ups here. So I don't mean to be taking it out on you all, but it's just a little frustrating to me.

I'm sorry, Mr. Otter.

Mr. OTTER. That's all right, Mr. Chairman. I'm the bottom of the political food chain here, and I understand that.

Mr. SHAYS. No. You were the one who helped illustrate the point.

Mr. OTTER. However, the chairman's recent observations and actions does bring me to my next question, which is what I was leading up to. We've spent $7½ million. We've employed eight agencies, or some assets from each agency, and the question is at what success rate. But more importantly to me is—the question would be who is in charge? Who is—you've got eight agencies. You've got $7.5 million being spent. Who is in charge here? I see—and I know, having been in business, but also been in government a long time, that there is conflicting areas of whose responsibility is what and turfy and all of that kind of stuff, but it seems to me that if this project was going after an issue which is as important as I believe it is, that we would have set ourselves up for success rather than a question of whether or not we've succeeded or failed.

So I want to know, Mr. Swartz, who is in charge?

Mr. SWARTZ. Well, Mr. Otter, in the narrowest sense, there is a charter group on which I sit.

Mr. OTTER. A group?

Mr. SWARTZ. A charter group.

Mr. OTTER. A group is in charge.

Mr. SWARTZ. That's correct——

Mr. OTTER. And how many is on that group?

Mr. SWARTZ. I would have to get you the exact numbers, though there's a representative from the law enforcement agency as well as the Department of Justice and the Department of State that sits on the charter group.

Mr. OTTER. What do you call this, a posse or what?

Mr. SWARTZ. No. That would be an interesting thing to call it, but charter group is the name of that oversight board.

With regard to the pilot project—and, again, I do want to emphasize that this was seen as a pilot project, and it is important to distinguish between the ADNET terminals and the actual creation of this network and the use of this network—or the terminals of this network for the Nigerian Crime Initiative. It is certainly the case, as the chairman suggests, there have been shifting in personnel over the years as agents come in and out, as people in the departments come in and out.

There are, of course, always competing objectives with regard to the fight of international crime, but I do want to indicate that the fight against Nigerian organized crime is broader than the particular initiative on ADNET, and certainly the chairman—we would be glad to provide anything that we've been provided by DISA or otherwise with regard to the initiative. We're certainly not trying to keep anything from the committee, either the successes or failures, but I think it is fair to say that the Department of Justice, at least, has not sat down with the new administration and made an assessment of how this has worked over the years it's been in place, and it's not been that long a period of time.

Mr. OTTER. How long has it been in place? When did you organize the charter group?

Mr. SWARTZ. The charter group, I believe, is 1998. So we're now reaching the end of the MOU period.

Mr. GILMAN. Would the gentleman yield?

Mr. OTTER. The gentleman yields.

Mr. GILMAN. President Clinton created that Executive order in 1996. It took 2 years to bring together a charter group?

Mr. SWARTZ. Well, I should say that the—and, again, the Secret Service can comment on this as well. The interagency group started working on the Nigerian problem long before that, and, in fact——

Mr. GILMAN. Forget Nigerian problem. How long did it take to follow President Clinton's Executive order and put together some oversight that the gentleman is asking about?

Mr. SWARTZ. Well, the response to PDD–42 extends far beyond the Nigerian Organized Crime Initiative. There are any number of working groups, I should stress, in any number of areas with regard to international crime. This is simply one aspect, one response——

Mr. GILMAN. But was there any oversight group appointed following that Executive order?

Mr. SWARTZ. Well, certainly the National Security Council did have an international organized crime coordination group that followed PDD–42 and that worked on coordinating these issues. As well, the Departments of Justice——

Mr. GILMAN. I thank the gentleman for yielding.

Mr. OTTER. I'm reclaiming my time.

Colonel Deacy, you obviously come from an environment which requires a chain of command. Do you feel comfortable operating in this kind of an environment?

Colonel DEACY. Sir, on this program or initiative, we are comfortable because we have a program. It's funded by the agencies involved. They validate what their requirements are through whatever means, in this case a group, and we take those and transform that into a solution that will technically do that. So for us there's no ambiguity or confusion.

Mr. OTTER. Obviously there is a lot for this committee, and obviously there is a lot for the intent what this committee had or felt that they had, because I'm not sure that we've come up with a success number here; 1 to 10, 1 being the worst, 10 being the best, in your estimation what has been your success since the charter group was formed and, I suspect, some sort of formal operations began?

Colonel DEACY. Sir, as the implementor of a solution, it's providing a tool. We really have no opinion on success or failure of how that tool is used so as a corporate opinion. We have none.

Mr. OTTER. I see. So you're not in charge?

Colonel DEACY. Certainly not.

Mr. OTTER. I'm still not sure who is, but I guess my overall question, then—perhaps I formulate this more as a statement, Mr. Chairman and members of the panel, than I do as a question, but why would we even entertain the thought of putting this same program into another theater of involvement when we don't know and we haven't achieved a level of what I would consider a measurable—or of success that we can at least brag on a little bit and say, this is what we've done?

The other thing that I'm really conflicted about here is I know there is sensitive information that you all gather, but it seems to me like somebody's criminal record would not be sensitive information, and that ought to be first line—that ought to be the first note, and that if the county sheriff of Lemhi County, ID wanted to find out what somebody from Nigeria—whether or not because of all those letter that is they sent, I'm sure, out to everybody, whether these people were legitimate, or did they have some kind of a criminal record, I would think that the irrigation superintendent ought to be able to get ahold of that.

Why is criminal information sensitive information? I do know that in most of the organizations that I've been a part of, knowledge is power, and that is what really concerns me here, and I don't like the idea of wasting $7½ million. And not only that, but taking agencies whose mission is required—could be required and utilized very effectively in other areas of operation and put them in on something that we've operated since 1990—had the permission to do since 1996 and operate since 1998, and I really can't get a grade. Could you give yourself a grade, Mr. Swartz; 1 to 10, 1 being bad, 10 being good?

Mr. SWARTZ. Mr. Otter, I think that the Department of Justice's perspective on this is that it is now time to think about a grade for the Nigerian Crime Initiative. We've had it in place. We've had it through the MOU period, and it's now time to assess where we stand.

Mr. OTTER. When you formulated the charter, did you and could you make available to this committee a list of achievable objectives for that? Did you expect to have certain successes on certain time lines, and if you did, could you make that available to this committee and what your success rate is there?

Mr. SWARTZ. I will certainly go back and see what the time line is. Certainly we did have objectives with regard to the number of terminals being put in place and the connectivity for those terminals. Those objectives have been met in that regard.

And I do want to stress that, again, I don't think this should be seen as money wasted, and it is money that has been spent to try and develop the concept, which hasn't been done before, of accessing each agency's data bases or a portion of those data bases on a particular crime area over a secure network. That in itself, I think, has been a useful experiment with lessons to be learned.

Mr. OTTER. I'm going to make you a deal, Mr. Swartz. Don't put words in my mouth, and I won't put words in yours. If I said "wasted," I misspoke, and I sincerely apologize for that. I said "spent." You said "wasted." That was your word.

Mr. SWARTZ. No. And I certainly didn't mean to suggest, Mr. Otter, that you said the money was wasted. I just don't want the committee to—the subcommittee to believe that it's——

Mr. OTTER. Thank you.

Thank you, Mr. Chairman.

Mr. SHAYS. Mr. Gilman, do you have some questions? Mr. Gilman, do you have questions you'd like to ask?

Mr. GILMAN. Well, again, from what we're hearing, it sounds like there is a need out there for some oversight besides the charter commission. Does the charter commission meet on a regular basis?

Mr. SWARTZ. The charter group has met on a regular basis. It is——

Mr. GILMAN. How often?

Mr. SWARTZ. It met at least, I believe, twice a year.

Mr. GILMAN. Twice a year.

Mr. TOWNSEND. Sir, the interagency working group has met every 4 to 6 weeks for the 12 to 14 months that I've been associated with the program.

Mr. GILMAN. Well, is that—Mr. Townsend, does that differ from the charter commission?

Mr. TOWNSEND. It does, yes. The interagency working group are below-policy-level players in the program; in other words, the people hopefully that are charged with making some things happen.

Mr. GILMAN. Well, the interagency working group, is there a primary assignment, the data exchange, the data sharing?

Mr. TOWNSEND. I would say that is not their primary assignment, although it is one key component; as I mentioned earlier, two sides to this, the ADNET component and the operational side. The Secret Service has been engaged in the operational side before PDD–42 in 1996. The Nigerian organized crime task forces that came about after the implementation of the interagency working group and the charter group or the second evolution of the Secret Service task forces that already existed.

Mr. GILMAN. When PDD–42 was issued, who had the responsibility, then, of formulating whatever implementation was needed? Mr. Swartz.

Mr. SWARTZ. My understanding is, Mr. Gilman, that the Attorney General had the lead in responding to international organized crime issues with regard to PDD–42, and certainly a number of steps were taken at that time to deal and expand our response to international organized crime. I would stress, as I have in the past, this is simply one part of the actions that the Department of Justice has taken against international crime.

Mr. GILMAN. Well, did PPD 42 prescribe the necessity for a central agency or central authority to implement it?

Mr. SWARTZ. I would have to review that. Again, I believe that the National Security Council, again, through its special coordination group, also took on a coordinating role. And I should say as well that PDD–42 did lead to the International Crime Control Strategy, which was subsequently promulgated, which I believe

this subcommittee has a copy of or which we can certainly provide. But that is as you are aware, that is quite a complete document that discusses a number of goals and objectives in combating international crime——

Mr. GILMAN. What is the title of that?

Mr. SWARTZ. This is the International Crime Control Strategy.

Mr. GILMAN. All right. And in that strategy, is there something about sharing data?

Mr. SWARTZ. Yes. It certainly does talk about interagency cooperation throughout, and I should say that this crime control strategy, crime currently in effect, is now under consideration by the administration for any revisions that do need to be made.

Mr. GILMAN. What was the date of that document?

Mr. SWARTZ. I believe it's May 1998.

Mr. GILMAN. And from the time that PDD–42 is issued, do you know whether any—was there any authorization or any implementation by any central agency of PDD–42?

Mr. SWARTZ. My understanding is, Mr. Gilman, that—well, of course, before PDD–42 and thereafter, there were a number of steps taken———

Mr. GILMAN. I'm talking about from the time the Executive order was issued in 1996.

Mr. SWARTZ. Well, my——

Mr. GILMAN. Would you tell me whether there has been any central authority implementing PDD–42?

Mr. SWARTZ. I think that the central authorities would be the Attorney General, and the National Security Council's coordination group would have been looking at the issues presented by PDD–42. But, of course, the Attorney General would have been working and meeting with her colleagues at the time.

Mr. GILMAN. All right. So National Security and Attorney General worked together. What did they do to implement PDD–42?

Mr. SWARTZ. I would be glad to supply to the committee any steps that were taken with regard to——

Mr. GILMAN. Would you do that and supply it to the chairman? Thank you very much.

Thank you, Mr. Chairman.

Mr. SHAYS. Ms. Barry, I'm——

Ms. BARRY. Yes, sir?

Mr. SHAYS. Bottom line, you're not inputting information—you're not providing input, but you can draw on this information. You would find it helpful, but you don't need top security clearance. In other words, you need something, share data, but just tell me your perspective again on——

Ms. BARRY. Our perspective is that we work in an unclassified environment overseas, and given the volume of cases we handle, we need a very, very quick response time.

Mr. SHAYS. Right.

Ms. BARRY. So basically the CLASS data base is name, date and place of birth of an individual and a code so when we get a hit, we know which agency to go to for the fuller report. So our officers in the field know enough in the first instance to suspend the case, with the general understanding of why they're suspending the case, and then working with headquarters back here and the other agen-

cies, we provide them the fuller information they need to make a final determination.

Mr. SHAYS. So——

Ms. BARRY. So we have a number of people at headquarters here who are reaching out to the law enforcement agencies on a regular basis.

Mr. SHAYS. Is your Department finding this a helpful system or not? What is your message to this committee?

Ms. BARRY. Our message to the committee is that we do, in terms of adjudicating visa cases, rely very, very much on Datashare, because—as I explained to Mr. Gilman, we're very satisfied with the program we have to identify potential terrorists. It's a very robust program. Because we don't regularly get information from the FBI out of the NCIC data base, we probably—we feel less successful in stopping individuals of concern for criminal activities, and we are working on that objective.

Mr. SHAYS. So your message to the committee is that you are a user of this system and would like to see it——

Ms. BARRY. We understand that tools for analysts to develop findings is very useful to us as the end user of the finding. So I can't speak for my colleagues who are analysts as to how effective ADNET has been per se as a tool, but we understand in general terms the use of tools for our work overseas.

Mr. SHAYS. Mr. Townsend, the—you described the New York office where you felt—you have 6 task forces, to go to 10, correct?

Mr. TOWNSEND. Presently, sir, we have 10 task forces, but not all of them have ADNET terminals. They have 10 task forces working—that focus primarily on——

Mr. SHAYS. Six have the terminals?

Mr. TOWNSEND. There are terminals in New York, Dallas, Chicago, Houston, Atlanta, Washington. The Baltimore task force terminal is expected late this year, and we'll also——

Mr. SHAYS. And we have terminals in other areas that are secured and so on?

Mr. TOWNSEND. Yes, sir. There are——

Mr. SHAYS. There have been 30?

Mr. TOWNSEND. There are terminals in Secret Service headquarters, FBI headquarters and so forth.

Mr. SHAYS. You describe the cooperation and involvement in New York. Tell me what type of participation you have in Houston and Atlanta.

Mr. TOWNSEND. Sir, in Houston, there are 14 Secret Service special agents full time assigned to the task force.

Mr. SHAYS. So that's one, the Secret Service. Now the other departments.

Mr. TOWNSEND. Postal Information Service has one. The FBI has one. The INS has one. And the rest are local officers.

Mr. SHAYS. So you don't have DEA, for instance, there.

Mr. TOWNSEND. We do not. And I'm sorry, Atlanta was the other one?

Mr. SHAYS. Yeah.

Mr. TOWNSEND. In Atlanta there are eight Secret Service, one INS, one Postal Inspection Service; and on an ad hoc basis, one IRS agent.

Mr. SHAYS. So no FBI and no DEA.

Mr. TOWNSEND. That's correct.

Mr. SHAYS. Why, when I asked you about the cooperation, why did you pick New York as the one you wanted to——

Mr. TOWNSEND. Well, it just happened to be first on my——

Mr. SHAYS. Because it's the one where you have the greatest cooperation, right?

Mr. TOWNSEND. Well, it's first on my list. That's what I looked at, yes, sir.

Mr. SHAYS. OK. I'm just trying to understand. And the task forces do what?

Mr. TOWNSEND. The task forces focus on operational issues and Nigerian crime. Reports come in in a variety of manners, either through the public, from local police officers, all the various ways crime gets reported. We target those cases, the criminal activity, that is, based on consultation with our task force partners, the U.S. attorney, or the district attorney, and make criminal cases.

Mr. SHAYS. Mr. Otter, you had a question you wanted to——

Mr. OTTER. Yes, Mr. Chairman.

I'm going to ask Mr. Townsend. I picked on you too much, Mr. Swartz.

Mr. Townsend, do you know if the organization has an organizational chart that you could supply the committee that kind of goes from the charter group to the interagency working group to kind of give us a flow of the information and a flow of control; and if we could center in on really who we could get these answers from, is there one person or two or three people, maybe, that we could get these answers?

Mr. TOWNSEND. Sir, I'll have to check and take for the record and supply to the committee if there is a chart with regard to the interagency working group.

I can tell you that in our task forces that operate—well, I shouldn't say our task forces. The task forces that the Secret Service hosts where the terminals happen to be located, they're organized along part military lines and squads and so forth, and we could provide that to the committee.

Mr. OTTER. So it would be a normal practice in the agency that you're involved in and with to establish an operations chart?

Mr. TOWNSEND. Well, I don't know——

Mr. OTTER. A chain of command or something.

Mr. TOWNSEND. Within the Secret Service, yes. I couldn't speak for the other agencies.

Mr. OTTER. Thank you.

That's all, Mr. Chairman.

Mr. SWARTZ. Mr. Otter, at the risk of——

Mr. OTTER. Oh. I guess I will pick on you.

Mr. SWARTZ. Certainly we can provide a list of the charter group members, of which I sit on their chair, as I said, and of the interagency working groups under the charter group. So we can provide that.

Mr. OTTER. Do you have an operations chart, an organizational chart of who is a part of it and what the chain—if there is a chain of command, what the chain of command is?

Mr. SWARTZ. I'm going to see if there is a chart per se. We certainly have a list of the members of the various working groups and who chairs those groups.

Mr. OTTER. Thank you.

Thank you, Mr. Chairman.

Mr. GILMAN. Mr. Chairman.

Mr. SHAYS. Sure.

Mr. GILMAN. Just one question of our good State Department representative. Let me just ask our counselor, Director who is here, and you've given a good—Catherine Barry, you've given a good insight to the problems you confront out there on the field. You say it was—wasn't until May that you finally were getting some decent exchange for your consular offices; is that correct?

Ms. BARRY. No, sir. We've had Datashare for many years to one degree or another. I'm not sure—oh, in May, I believe I said we've replicated data back here.

Mr. GILMAN. In your testimony, you're saying for the first time since May, you're beginning to get a decent exchange between the main office and your office. I think I saw that in your testimony. But at any rate, you're making some recommendations. You're saying Customs is taking steps to share their serious violator data. How far along are they with that—taking the steps to do that?

Ms. BARRY. One moment, please, sir.

Sir, we have an agreement in principal with Customs. We are discussing technical issues at this time to finalize our agreement.

Mr. GILMAN. How long will it take to iron those out?

Ms. BARRY. I can't estimate at this time, sir. I'll take the question, if you—if you're willing——

Mr. GILMAN. Well, if it can be of assistance in expediting that, we'd welcome your telling us if you're running into any roadblocks or delay.

Ms. BARRY. I certainly appreciate that, sir. We view this, as I said, as simply technical people getting down and figuring out how the data shall actually be accomplished, but——

Mr. GILMAN. Then you're also saying Consular Affairs already exchanges data with DEA, but we want to improve the efficiency of that exchange closer to real-time rather than a slower tape exchange. What is taking—has the problem been in that delay?

Ms. BARRY. Again, sir, it is a technical issue on the interface that the two agencies would use to accomplish that. For further details, I would have to take the question. I am the worst person in the word to explain technical issues.

Mr. GILMAN. Who is your assistant that is giving you the information? Do you want to come to a mic and identify yourself?

Mr. BRENNAN. Mr. Gilman, I'm John Brennan. I am with the visa office. I work for Catherine Barry and the interagency——

Mr. GILMAN. Right. What is taking so long to iron out these interagency problems?

Mr. BRENNAN. Well, it's really not taking very long, in the sense that we only just started discussions in the past couple of months with DEA as to establishing an electronic means to do this. So there is no real delay. We expect it to work out in a reasonably timely fashion.

Mr. GILMAN. All right. Could you specify for this committee any of those technical difficulties that may be delaying an adequate change of information and see if we can be of any help to you?

Mr. BRENNAN. OK, sir. I will.

Mr. GILMAN. Now, in——

Mr. SHAYS. Excuse me. I just want to interrupt. Would you identify yourself for the record, again, and give your card to the transcriber here?

Mr. BRENNAN. Certainly I will. My name is John Brennan. I'm in the Department of State in the visa office and the interagency systems liaison unit of the visa office.

Mr. SHAYS. And if you would, make sure that you—and I want you to know that you have the same status as Senator Byrd. I have sworn in Senators, Cabinet officials, Members, and the only one I chickened out was when Senator Byrd came, I couldn't swear him in, and you're the second one. So you will now carry that status. Two people in my 7 years have spoken before this committee and not been sworn in.

Mr. BRENNAN. I apologize for that breach of etiquette.

Mr. GILMAN. Please don't leave the mic yet.

Ms. Barry said, in regular consultations with the INS, we're working to upgrade this——

Mr. SHAYS. I'm going to ask the gentleman just to raise his right hand.

[Witness sworn.]

Mr. SHAYS. Thank you. Let me just explain that when we do swear in people, we swear in everyone so someone doesn't say, why me and not someone else? And, you know, obviously we don't always need to swear someone in, but this way we cover it. Thank you. I'm sorry.

Mr. GILMAN. Thank you, Mr. Chairman.

Ms. Barry said in regular consultations with INS, we're working to upgrade Datashare to ensure Lookout data quality and improve the speed of transmission of departure and deportation. Is there any reason why that is being delayed?

Mr. BRENNAN. We have Datashare mechanisms that work with INS at—some of them at virtually real-time speed, but INS also has many layers of data within it, and the layer at which we take data, the interagency border inspection system, doesn't always contain all the data that INS has that we would like on a timely basis. So we're working with INS to get some other portions of data that it has, for instance, data on people who are being deported, added to their systems, either added to the interagency border inspection system more quickly or provided to us in some other manner so that we will have it available more quickly. It's a timing matter mostly.

Mr. GILMAN. It's Mr. Brennan, right?

Mr. BRENNAN. Yes, sir.

Mr. GILMAN. Mr. Brennan, if you would again notify our committee of anything we can do to expedite those problems. If it's a need for more equipment or cutting through some of the red tape, we'd welcome knowing about that.

Mr. BRENNAN. Very good. I might add there's really not a need for more equipment. We're in pretty good shape in that regard.

Mr. GILMAN. And then Ms. Barry went on to say, we believe interagency data sharing, when more fully deployed, will very effectively deter aliens who are counterfeiting documents and making fraudulent items.

Is there something we can do to make this more effective?

Ms. BARRY. Well, sir, we're very pleased with the initial results of the replication of data, because everyone's data is now feeding into Washington, and Washington is making it available to officers overseas. And we've begun a pilot with INS. If you are in Paris talking to an individual, and you have some concerns about the quality of the visa that he's shown you, you can now make a query and look at the original visa issued in Bangkok, let's say, compare the photo of the original visa with the individual standing in front of you, the name as specified in the original visa with the name as it now appears on the document. So we are capturing look-alikes, imposters and people who have somehow fiddled with the information on the original visa in a much more effective manner.

Mr. GILMAN. Ms. Barry, you went on to say, since ADNET is a compendium of law enforcement data, wouldn't this tool be useful in each visa unit overseas? What prevents that from happening?

Ms. BARRY. Primarily because we're in unclassified workspace. We could not have access to sensitive law enforcement data——

Mr. GILMAN. Mr. Swartz, what can we do to improve that situation?

Ms. BARRY. If I may finish?

Mr. GILMAN. Go ahead. I'm sorry.

Ms. BARRY. I'm sorry, Mr. Gilman. Other members of the U.S. mission overseas may, in fact, have access to sensitive information, and through the country team mechanism and other coordinating mechanisms of an Embassy, consular officers can consult sensitive information through—with the help of their colleagues.

Mr. GILMAN. That sounds a little complicated and burdensome and time-consuming.

Mr. Swartz, what can we do to assist our consular people who are out there on the front line to screen the people we don't want coming into the country?

Mr. SWARTZ. One thing, Mr. Gilman, that the Nigerian Organized Crime Initiative has done through ADNET is placed five ADNET terminals in two locations in foreign countries in——

Mr. GILMAN. Again, concentrating on Nigeria, we're talking about across the board, throughout the world.

Mr. SWARTZ. Yes. I certainly understand that. The way it would have to be done to make use of ADNET would be to have a similar program of either placing ADNET terminals in our consulates or Embassies.

Mr. GILMAN. But what can we do to accomplish that?

Mr. SWARTZ. That, I believe, would be a question really of State Department's availability and funding.

Mr. GILMAN. Well, I don't know. Is it just funding, or is there some restriction? Ms. Barry?

Ms. BARRY. I think we're talking about a methodology of working a case. What we're trying to give consular officers is a name check system that is very robust. But——

Mr. GILMAN. Well, ADNET would help you with that, wouldn't it?

Ms. BARRY. The name check is only the name, the identifying name, and date and place of birth and a simple code to explain that it's somewhat of concern. The follow-on information does come differently and needs to come differently, because otherwise we would slow down the entire visa adjudication function.

Mr. GILMAN. But ADNET would help you do that; would it not?

Ms. BARRY. Our methodology is to suspend a case of concern and then take the time we need to adjudicate that, using all the tools available to us.

Mr. GILMAN. How effective has been your visa VIPER program to proactively get the names of the bad guys into the data base system for visas?

Ms. BARRY. We certainly routinely receive submissions from country teams around the world for visa's VIPER there is a requirement that every post respond—report one way or the other on a quarterly basis.

Mr. GILMAN. And has it been effective?

Ms. BARRY. I believe so, sir. We have many names in the data base based on visa's VIPER submissions.

Mr. GILMAN. Now, Mr. Swartz has said to get the ADNET available to you, that's up to the State Department. Is there any restriction on your getting that kind of a system put in place?

Ms. BARRY. My colleagues in the Bureau of Diplomatic Security do have access to ADNET. I would have to take the question for further comments from them and——

Mr. GILMAN. Would you do that?

Ms. BARRY. Yes, I will.

Mr. GILMAN. And let us know if there's any restriction or obstruction for utilizing ADNET in your consular offices.

Thank you very much. And thank you, Mr. Chairman.

Mr. SHAYS. Mr. Schrock.

Mr. SCHROCK. I'm just trying to get caught up.

Mr. SHAYS. I was thinking that, and I do have a quick question or two. Is it fair to say that NCI is the first attempt to share law enforcement data on one system? Is that fair to say, Mr. Swartz?

Mr. SWARTZ. I believe that's correct, Mr. Chairman.

Mr. SHAYS. And from my standpoint—and I admit it's somewhat of a superficial look, but it logically says, well, that makes a lot of sense. We used obviously a case in which Nigeria seemed to interface with so many different agencies, so we had task force—we had ADNET before NCI. ADNET was a system in place.

Mr. SWARTZ. That's correct.

Mr. SHAYS. NCI then basically—we had task force before we had ADNET NCI.

Mr. SWARTZ. That's correct.

Mr. SHAYS. And we kind of combined the two. So I figure there are two circles. There's ADNET, and there's NCI, and they kind of overlap, and we've got this thing. And we're kind of—I'm wondering and my staff is wondering if these circles aren't kind of going in this direction.

From my standpoint, I would almost give a congressional Medal of Honor to some—I guess it's called a Medal of Honor to someone

who could get the different law enforcement organizations to share data. I mean, when you get the FBI and the DEA and the Secret Service and to some extent INS, everybody willing to share data, boy, hats off to the person who can do that.

So, you know, I consider this a big deal. I mean, I consider—but—so I guess what I want to understand—maybe, Mr. Townsend, you could respond—tell me—maybe it's the obvious, but tell me why there is a reluctance; why is it like pulling teeth? It's not something that someone runs to the dentist's office to do, right? It sounds like there's—why do people have to be made to do what seems logical?

Mr. TOWNSEND. Well, I think, Mr. Chairman, that there is a lot of information sharing going on, and I don't mean to answer your question by saying there's not a lot of room for improvement. There is. Law enforcement is somewhat unique with regard to information sharing. There are source issues. There are issues with regard to undercover personnel, issues that those of us who work in that environment and have worked in that environment hold close to our hearts and take it very seriously. Clearly your point is well taken.

In the law enforcement system which we have decided that's best for our country—that is, one which has many different Federal agencies and some thousands upon thousands of local agencies, as opposed to the model where there's one national police force and perhaps no local agencies—this is one of the consequences of that. Not that we shouldn't do better. We can do better. But there are—it is an extremely complex issue.

Mr. SHAYS. Yeah. It is extremely complex, and I'm trying to—I guess in one way it's very simple, in one sense, but I'd almost felt like I need to filibuster, because I don't want this hearing to end before I have a sense of a handle on this. I was thinking if I were you, Mr. Swartz, I wonder—all of you kind of gave your—kind of some details about the program and how it's working, and I'm wondering if I were in your shoes, if I wouldn't have come in and said, this is an extraordinary program. It's exciting in terms of its potential. We've had some successes, some failures. We've really succeeded in doing this, but we've failed to do this. And I would have thought, Mr. Townsend, you would have done almost the same thing; really great success, a failure here, this is what we're working on. So I get the sense that there's really not a buy-in yet to this, and there's not a sense that the program is working all that well.

Mr. TOWNSEND. May I respond, Mr. Chairman?

Mr. SHAYS. Sure.

Mr. TOWNSEND. With regard to the Secret Service and the Nigerian crime issue, there certainly is an agency buy-in. We were among those, as I mentioned in my oral statement, that identified the issue of Nigerian crime in the 1980's, and not to diminish the efforts of our Federal law enforcement partners and our State law enforcement partners, but certainly we have been among those at the forefront, and I think everyone would agree with that assessment.

So there certainly is a commitment, and there are successes, which I have available for the committee, should you care to hear

them now, or for the record. Operationally, there are successes out there. We are making cases that make a difference and the U.S. attorneys in their districts want to have and that real people are affected by. So the Secret Service, you know, is committed to the program. There are—I mean, there are issues. It's a complex situation.

Mr. SHAYS. But, you know, let me ask you, why is it complex?

Mr. TOWNSEND. Well, sir, I think to some degree for the things I have stated, I mean, we are a country with a variety of law enforcement agencies, and these are very real——

Mr. SHAYS. Just take the Federal. Why is it complex for the Federal Government to work together to share data that could help get at terrorists, help get at criminals, help make sure that people don't get in this country, shouldn't get into this country?

Mr. TOWNSEND. I have no quibble with that, sir.

Mr. SHAYS. OK. Why do I say that's—I mean, I did say it earlier that it's complex, and I was trying to give my excuse, because I feel so—I don't feel that I'm getting it. So I like to think it's complex and that I'm not dumb.

Anyway, I still don't understand why it's complex.

Mr. TOWNSEND. If I may?

Mr. SHAYS. Sure.

Mr. TOWNSEND. With regard to the Secret Service, we have uploaded the entirety of our master central index with regard to Nigerian crimes since the start—every 30 to 60 days.

Mr. SHAYS. OK. So by complex, it's just a hell of a lot of to work to get that done into the data system. You've got to put this information into the system so others can access it.

Mr. TOWNSEND. It was a lot of work, which we accomplished and continue to accomplish.

Mr. SHAYS. I agree with that, but complex would not be the word I described, but pain in the neck or something stronger, taking resources from another place, all of those things I agree with; complex, no.

Mr. SWARTZ. If I may, Mr. Chairman. One additional complexity does arise when you go beyond the index system that Secret Service has put on, and I think Mr. Townsend referred to this already. In one document that the—one of the NCI documents that was produced, I know, to the subcommittee, there's a list of the steps that have to be taken by each law enforcement agency once it's moving toward full text loading of documents, which is what the FBI and some other agencies have done. And there—again, for some of the reasons that Mr. Townsend is suggesting, you do begin to reach new levels of complexity because of grand jury secrecy rules, protection of sources, limitations on how to——

Mr. SHAYS. OK. So what document you can provide, then that becomes some—that does get into—the complexity——

Mr. SWARTZ. Right. Which I think goes back to the earlier discussion that was held with the subcommittee earlier today with regard to how this should move, whether——

Mr. SHAYS. Some information that just simply is not going to be provided, so no one should think it's comprehensive. There's some information privacy issues, some documents that may be classified,

some documents that—well, some classified documents can go in there, obviously.

Mr. SWARTZ. Yes. I think that buy-in, though, from the agencies turns in part on the amount of time and resources that are being expended for that kind of getting of complete, full text records, as opposed to an index system, and I think that is one of the things that the Department of Justice will look at for data sharing in the future.

Mr. SHAYS. Right. And I would accept this if you said, you know, it takes a lot of—it takes valuable time in order to do this; it's a money question, and so on. Those are helpful to us. Saying it's complex prevents me from understanding. Explaining why it's difficult, explaining that there are financial challenges, explaining there are manpower, then that's an instructive, educational and believe it—you know, if you tell us the truth, then actually we might do something intelligent, and that's helpful. Thank you.

Mr. Schrock, do you—I'm kind of done.

Mr. Gilman, I really appreciate your questions. Are you all set? Is there any question that you would like to respond to?

Mr. Deacy, is there anything you'd like to say, or Ms. Barry, in the conclusion?

Colonel DEACY. No, sir.

Mr. SHAYS. Well, we appreciate you all being here, and we'll get a handle on this, and I thank you for helping us in that process. This hearing is adjourned.

[Whereupon, at 11:45 a.m., the subcommittee was adjourned.]

○