AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

S. Hrg. 110–1028

INFORMATION SHARING: CONNECTING THE DOTS AT THE FEDERAL, STATE, AND LOCAL LEVELS

HEARING

BEFORE THE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS UNITED STATES SENATE

ONE HUNDRED TENTH CONGRESS

SECOND SESSION

JULY 23, 2008

Available via http://www.gpoaccess.gov/congress/index.html

Printed for the use of the
Committee on Homeland Security and Governmental Affairs

U.S. GOVERNMENT PRINTING OFFICE

44–580 PDF WASHINGTON : 2010

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) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

JOSEPH I. LIEBERMAN, Connecticut, *Chairman*

CARL LEVIN, Michigan
DANIEL K. AKAKA, Hawaii
THOMAS R. CARPER, Delaware
MARK L. PRYOR, Arkansas
MARY L. LANDRIEU, Louisiana
BARACK OBAMA, Illinois
CLAIRE McCASKILL, Missouri
JON TESTER, Montana

SUSAN M. COLLINS, Maine
TED STEVENS, Alaska
GEORGE V. VOINOVICH, Ohio
NORM COLEMAN, Minnesota
TOM COBURN, Oklahoma
PETE V. DOMENICI, New Mexico
JOHN WARNER, Virginia
JOHN E. SUNUNU, New Hampshire

MICHAEL L. ALEXANDER, *Staff Director*
CHRISTIAN J. BECKNER, *Professional Staff Member*
BRANDON L. MILHORN, *Minority Staff Director and Chief Counsel*
JOHN K. GRANT, *Minority Counsel*
TRINA DRIESSNACK TYRER, *Chief Clerk*
PATRICIA R. HOGAN, *Publications Clerk and GPO Detailee*
LAURA W. KILBRIDE, *Hearing Clerk*

CONTENTS

	Page
Opening statements:	
Senator Lieberman	1
Senator Pryor	20
Prepared statement:	
Senator Voinovich	35

WITNESSES

WEDNESDAY, JULY 23, 2008

Eileen R. Larence, Director, Homeland Security and Justice Issues, U.S. Government Accountability Office	4
Hon. Thomas E. McNamara, Program Manager, Information Sharing Environment, Office of the Director of National Intelligence	6
Charles E. Allen, Under Secretary for Intelligence and Analysis and Chief Intelligence Officer, U.S. Department of Homeland Security	9
James M. Thomas, Commissioner, Department of Emergency Management and Homeland Security, State of Connecticut	12
Jeffrey H. Smith, Partner, Arnold and Porter	15

ALPHABETICAL LIST OF WITNESSES

Allen, Charles E.:	
Testimony	9
Prepared statement	129
Larence, Eileen R.:	
Testimony	4
Prepared statement	36
McNamara, Hon. Thomas E.:	
Testimony	6
Prepared statement	59
Smith, Jeffrey H.:	
Testimony	15
Prepared statement with an attachment	149
Thomas, James M.:	
Testimony	12
Prepared statement	145

APPENDIX

"Annual Report to the Congress on the Information Sharing Environment," prepared by the Program Manager, Information Sharing Environment, June 2008, submitted by Mr. McNamara	64
Questions and responses for the Record from:	
Ms. Larence	164
Mr. McNamara	166
Mr. Allen	168

INFORMATION SHARING: CONNECTING THE DOTS AT THE FEDERAL, STATE, AND LOCAL LEVELS

WEDNESDAY, JULY 23, 2008

U.S. SENATE,
COMMITTEE ON HOMELAND SECURITY
AND GOVERNMENTAL AFFAIRS,
Washington, DC.

The Committee met, pursuant to notice, at 10:05 a.m., in room SD–342, Dirksen Senate Office Building, Hon. Joseph I. Lieberman, Chairman of the Committee, presiding.

Present: Senators Lieberman and Pryor.

OPENING STATEMENT OF CHAIRMAN LIEBERMAN

Chairman LIEBERMAN. Good morning and welcome to today's hearing, "Information Sharing: Connecting the Dots at the Federal, State, and Local Levels."

I want to say at the outset that Senator Collins called and, unfortunately, there has been a crisis in Maine, and so she cannot be with us today. But she will certainly follow the transcript and the statements that you make.

The attacks of September 11, 2001, obviously showed us how disastrous it can be when intelligence information gathered by one agency is not shared with other agencies—Federal, State, and local—who share the responsibility to protect our Nation and our people.

The 9/11 Commission Report documented instance after instance where agencies either kept crucial information to themselves or, even if they were prepared to share the information, did not let other agencies know they had it. Because of this information hoarding, crucial clues that existed in different databases that, if combined and analyzed, might well have thwarted or stopped those attacks were missed, and the terrorists succeeded in the most devastating attack on the United States since Pearl Harbor.

The 9/11 Commission wrote in its report, "The culture of agencies feeling they own the information they gathered at taxpayer expense must be replaced by a culture in which the agencies instead feel they have a duty to the information"—to share the information—"to repay the taxpayers' investment by making that information available."

In today's hearing we will examine progress on information sharing since then. In fact, this is the first Committee inquiry since 2004, our first round of post-9/11 Commission Report hearings on

this subject. And so we are going to ask in simple terms what has improved and what still needs to be improved.

We have a panel of very distinguished and experienced witnesses, and I welcome you all here today and thank you for being here.

Charlie Allen is—I have used so many superlatives to describe you. I think I should just say "Charlie Allen." I was once at a meeting a couple years ago where Henry Kissinger was introduced by somebody as "a man who needed no introduction." So Dr. Kissinger got up and said, "It is probably true that I need no introduction, but I like a good introduction." Anyway, you are a national asset, Mr. Allen, and I thank you for being here.

I also particularly want to welcome Skip Thomas, Commissioner of the Department of Homeland Security from Connecticut, who is here to talk about some of the very innovative work being done, I am proud to say, in my home State.

We also are very glad to have Ambassador McNamara, Program Manager of the Information Sharing Environment; Jeff Smith, former General Counsel of the CIA, now a partner at Arnold and Porter, who worked with our Committee on the intelligence reform legislation and was very helpful; and Eileen Larence of the Government Accountability Office (GAO).

In the testimony today, I am pleased to say we are going to hear about significant progress over the last few years to improve the sharing of critical information across Federal agencies, and between Federal, State, and local agencies. And I thank you for that.

Following hearings of our Committee in 2004, which I referred to, Congress passed and the President signed into law the Intelligence Reform and Terrorism Prevention Act, which created the Office of the Director of National Intelligence (ODNI) to forge a greater unity of effort among our country's very diverse intelligence community. The legislation also established the National Counterterrorism Center (NCTC) and the Office of the Program Manager for the Information Sharing Environment (ISE), both intended to strengthen and streamline the exchange of terrorism-related information within the Federal Government.

The 9/11 Commission Act, which we call "9/11 II," signed into law last year, further enhanced the authorities of the Information Sharing Environment program manager and established in statute the State and Local Fusion Center program office at the Department of Homeland Security.

At the National Counterterrorism Center, officials from a wide variety of agencies—CIA, FBI, NSA, DHS, DOD, and many others—now work side by side, 24/7, to assess terrorism-related evidence, indications, and warnings and, of course, to jointly analyze the threat. The NCTC is now the one place where our government is responsible for connecting the dots that were left dispersed prior to September 11, 2001. And it is quite a remarkable achievement, and I am sorry Senator Collins is not here because we both have been there. It is one of those moments in the Senate life when you actually see something that you helped to create created and feel the satisfaction and encouragement to know that it is really making a difference. Those moments do not come too often, but when they come, they are quite satisfying.

State and local governments are now also increasingly seen as partners by the Federal Government, and the network of fusion centers across the country, with support from the Department of Justice and the Department of Homeland Security, is playing a valuable role in the broader efforts to share terrorism-related information and to detect suspicious activities.

Just last month, fusion centers from Indiana and four other States collaborated on a joint assessment that looked at suspicious activities related to a certain sector of public infrastructure, and they did so acting on their own initiative.

This kind of horizontal, decentralized information sharing and analysis is exactly the kind of activity that we had hoped the fusion centers would be doing. It fixes one of the information-sharing gaps that was evident as we looked back at the September 11, 2001 plot, where Federal agencies did not connect the dots regarding those suspicious activities at flight schools in various parts of the country.

However, as we will discuss, more work remains to be done to fulfill the 9/11 Commission's charge that our security and intelligence agencies change from a culture of "need to know" to a culture of "need to share."

GAO has included this subject matter, which they call "Establishing Appropriate and Effective Information-Sharing Mechanisms to Improve Homeland Security," on its high-risk list since 2005, not that there has been no progress made. There obviously has, but I think it is a measure of the very high consequences of failure, unacceptably high, and how critical it is that all relevant agencies continue to work to remove this item from the high-risk list.

As we are going to hear from GAO, the Program Manager for the Information Sharing Environment, according to GAO, really needs to create a road map so that it can objectively monitor progress, ensure accountability, and make participating agencies aware of their distinct responsibilities as part of the Information Sharing Environment.

Without that kind of a road map, it is going to be very hard to identify and root out remaining cultural, organizational, or technological barriers to effective information sharing that we know still exist.

We do not want to allow the continuation of institutional stovepipes that funnel intelligence straight up a single agency rather than a decentralized, networked approach, where information is broadly distributed.

I think we need to build on the considerable progress that has been made. That is what I take away from the work that has been done and my understanding of it. Unfortunately, there are some, I gather, who would like to see the Information Sharing Environment program office defunded and disbanded by as early as 2010 and then apparently return to the old ways of doing business, which obviously simply did not protect the security of the American people. I want to make clear this morning my firm opposition to any such move. I will do anything I can to stop it from proceeding.

So I look forward at this moment, as we approach a transition in government, to working with the next Administration in making these programs that are so critical to our Nation's security even

more efficient and effective, and the work that all of you have done, to prepare for this morning's hearing will certainly assist this Committee in doing so. Thank you very much.

Now I would like to call first on Ms. Eileen Larence, who is the Director of Homeland Security and Justice Issues at the U.S. Government Accountability Office. Thanks for being here.

TESTIMONY OF EILEEN R. LARENCE,[1] DIRECTOR, HOMELAND SECURITY AND JUSTICE ISSUES, U.S. GOVERNMENT ACCOUNTABILITY OFFICE

Ms. LARENCE. Thank you, Mr. Chairman. Thank you for the opportunity to summarize the results of our recent reviews of the government's efforts to better share terrorism information since September 11, 2001. As you already acknowledged, in 2005, GAO did place the issue of information sharing for homeland security on its high-risk list, and it has been monitoring efforts to remove barriers to sharing since then. My testimony this morning summarizes our recent work on: One, assessing the status of the Information Sharing Environment, called for in the 2004 Intelligence Reform and Terrorism Prevention Act; two, challenges to State and local efforts to create and maintain fusion centers; and, three, recent reforms to streamline rules for handling sensitive information.

In the 7 years since September 11, 2001 and the 4 years since the intelligence reform act, Federal, State, and local agencies are clearly sharing more terrorism information. New organizations were created and new processes, systems, and networks evolved to handle the sharing, and the Congress and Administration issued new laws, policies, guidance, and standards to promote more sharing. But there is still critical work that the program manager for the Information Sharing Environment and agencies must do, as you also acknowledged. They need to better integrate these pieces, continue to overcome agency stovepipes and change cultures that promote information protection over secure sharing, better monitor and measure progress, and perhaps most importantly, maintain momentum.

In a report we are releasing to you today, GAO acknowledges that building the environment is a very complex challenge involving many stakeholders, each with equities and investments already in place. Nevertheless, the program manager and agencies have had a measure of success. The program manager issued an implementation plan in 2006. He initiated a governance structure and working groups. His office and agencies achieved most of Phase 1 of the plan, which focused on setting up and getting ready for implementation. This included developing information inventories and directories, uniform standards, and a technology framework.

The program manager is also leveraging initiatives agencies independently pursued, such as terrorist watchlisting and fusion centers, and he has issued two annual reports that begin to catalogue these actions and measure progress. But progress has been tempered, to some extent, by several gaps to fill.

First, the program manager and Federal agencies key to making the environment work—and that includes the Departments of De-

[1] The prepared statement of Ms. Larence appears in the Appendix on page 36.

fense, Homeland Security, Justice, and State—still have to fully define the environment's scope and parameters or what it is to achieve and how it will operate. This includes what information all critical stakeholders need to combat terrorist threats, what information should be shared, how it will be made available to analysts, while also protecting it as well as civil liberties, and what technologies will be used.

Second, work on the environment has pushed agencies to partner better on information sharing, but there is still some confusion and conflict about agency roles, responsibilities, and level of commitment versus that of the program manager that need to be resolved because of such slow progress. And questions remain as to whether the program manager has the authority needed to drive change and who is holding agencies accountable.

And, third, the program manager and agencies have made good-faith efforts to set and refine goals, objectives, and metrics to design the environment. But taken together, these efforts do not yet provide a complete and current road map and accountability systems to guide future implementation and investments, even though the hardest part of building the environment is still to come.

The 2006 plan's milestones were ambitious. It is unclear what has replaced it to guide agencies all in the right direction. Developing these tools is important to give this clear sense of future direction and priorities, and to measure how far we are in setting up the environment, as well as how much sharing has improved and what is left to achieve.

Turning now to the issue of State and local fusion centers, our work on such centers showed that they vary widely but face some similar challenges. The Federal Government is helping to address these challenges, but they are not yet resolved. States and localities created centers to fill information gaps the Federal Government could not. The centers range in maturity and capability. Most focus on collecting information on all crimes or all hazards, not just terrorism; and most of it is collected by law enforcement entities, but partnered with many other State and local agencies and have Federal personnel assigned.

A number of centers reported challenges: Having to manage too much information and too many systems; finding specific operational guidance and analyst training; finding and keeping qualified personnel; negotiating the Federal grant process; and of most concern, sustaining center operations long term.

DHS and DOJ are helping to address these challenges by providing people, guidance, technical assistance, training, system access, and grant funding. But we recommended that the Federal Government better determine the long-term support it expects to provide these centers. The Administration addressed this to an extent in the 2007 National Information Sharing Strategy. In addition, provisions in the 9/11 Commission Act address support for fusion centers. And a new bill to remove grant restrictions on personnel funding addresses a concern centers also voiced.

Finally, in regard to protecting sensitive information, in March 2006, we reported that agencies were using a myriad of different labels to designate information as sensitive but unclassified, as well as confusing and conflicting rules about handling it, thereby

discouraging some sharing. We recommended that the government streamline these practices. The President recently issued a policy calling for the use of a uniform controlled and classified information label and providing several options for handling dissemination. This is a good start. But as our work demonstrated, it will be important to ensure individual agencies have their own guidance with specific examples as well as training to help employees determine what information should bear this label. They will also need an effective set of internal controls, such as supervisory review and audits, to ensure employees make accurate decisions so as not to inhibit sharing.

Mr. Chairman, this concludes my statement, and I would be happy to answer any questions.

Chairman LIEBERMAN. Thanks very much, Ms. Larence. Good beginning.

Ambassador McNamara, welcome. You are next.

TESTIMONY OF HON. THOMAS E. MCNAMARA,[1] PROGRAM MANAGER, INFORMATION SHARING ENVIRONMENT, OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

Mr. MCNAMARA. Thank you, Mr. Chairman, and I would like to thank you and the Committee for the opportunity to be here with the other members of the panel to talk about the progress in terrorism information.

Just over 2 years ago, I was appointed program manager for the Information Sharing Environment (ISE) with a clear mandate defined by statute and the presidential directives to improve the sharing of terrorism-related information among those responsible for protecting our Nation from attacks. There was much to do and much pressure to move quickly. We had, however, no Information Sharing Environment to use as a model. No precedents existed, at least not in government.

My charge was not to create the Information Sharing Environment from scratch. Instead, the Congress and the President instructed me to work with others at all levels of government to build and expand on existing communication and sharing capabilities.

I am pleased to report that priorities were set, initiatives were taken, and collaboration has been the hallmark of this effort. We have accomplished a great deal in a short period of time. We have defined the path to be taken in establishing the ISE. The Information Sharing Implementation Plan and the President's strategy outlined that path.

The initial functioning of the ISE is underway, and it is beginning to have an impact on how the government does business. This is the beginning of a cultural transformation that if it is continued for an extended period, can make the ISE a routine and necessary part of government functioning.

Our second Annual Report to the Congress is very specific about how information sharing has improved through our efforts. And by "our," I mean the Project Managerof the Information Sharing Environment (PM–ISE) office that I head, the Information Sharing Council agencies that have worked on this, the Office of Manage-

[1] The prepared statement of Mr. McNamara appears in the Appendix on page 59.

ment and Budget (OMB), the White House, our State, local, tribal, and private sector partners above all, and this Congress—all of whom have worked in partnership to bring about these accomplishments.[1]

I want to quickly list and highlight just a couple of the changes that I think are important. There are many more.

The first, sharing with State and locals. A framework for sharing information among Federal, State, and local and tribal governments and the private sector is being implemented. The framework is designed with substantial input by State and local officials. We consulted with them. I want to highlight just two areas that are a very high priority. The one is that we have a functioning Interagency Threat Assessment and Coordination Group now established and operating in the NCTC. This brings together Federal, State, and local partners and personnel who work side by side in developing and producing intelligence products that are specifically designed for State and local consumers, a first in the Federal Government.

Second, we have laid the foundation for a national network of State and major area fusion centers. This network is functioning at a very preliminary stage now, but it is getting stronger by the day and by the month. Today, there are over 50 fusion centers in operation nationwide. DHS, FBI, and other Federal agencies have personnel in many of these centers, and these centers are being connected to classified and unclassified Federal information systems.

The second area was already mentioned by our colleague from the GAO. The President has issued a new standardized procedure for handling the otherwise chaotic jumble of information known as "sensitive but unclassified." This new regime, called Controlled Unclassified Information came about as a result of the work of the Office of the PM–ISE and several of the agencies on the Information Sharing Council.

Protecting privacy and legal rights. This has from the very beginning been at the top of our agenda. There are now Information Sharing Environment privacy guidelines, there are implementing procedures for those guidelines, and there is a user's manual for Federal agencies to use to ensure that all the activities taken in the context of the Information Sharing Environment protect the information privacy rights and other legal rights of Americans. Every agency has a designated senior privacy officer, and we have an ISE Privacy Guidelines Committee. Most of those privacy officers sit on that committee. We are working with our partners to see if we cannot come up with a common way to incorporate those privacy guidelines in the rules and regulations that govern State and local information sharing.

Finally, Suspicious Activity Reports (SAR). You mentioned this, Senator. We are implementing a standardized process for sharing information related to these suspicious activities by State and local authorities. It will help to detect terrorists operating in our local communities while at the same time ensuring that the information, privacy, and other legal rights of Americans are protected. This

[1] "Annual Report to the Congress on the Information Sharing Environment," June 2008, submitted by Mr. McNamara appears in the Appendix on page 64.

standardized, mostly common approach is being implemented over the next year in a pilot program. And I want to commend at this point the Los Angeles Police Department and its chief, William Bratton, for the foundational work that they have done to create a SAR model that can be replicated by other localities. And I also want to commend the Bureau of Justice Assistance, the Major City Chiefs Association, and the International Association of Chiefs of Police that are working closely with the LAPD and with my office to incorporate the LAPD process into our pilot program. We are listening to the State and local authorities.

Although I am pleased with the progress we have achieved, I am not suggesting we have finished the job. Far from it. The ISE is functioning, albeit haltingly, and not at all in some areas. But we have laid the basis for a fully functioning ISE in the future. We are, to use Churchill's famous phrase, "at the end of the beginning."

The challenges to the Information Sharing Environment are not to be underestimated. Information silos, cultural habits, budget limitations, bureaucratic inertia, and other barriers that inhibit sharing are very strong, and they are impeding progress. The progress I have described today in my oral and written testimony has been a hard one. It is unfinished, definitely. It must be developed further and then institutionalized and ingrained in our work cultures if it is to be a long-term implementation.

I would point out that the real power to implement, however, rests with the major Federal departments whose planning and budgets are not yet focused on the ISE. As program manager, I have sought to champion interagency collaboration to build that Information Sharing Environment. In doing this, there are three characteristics that have been critical to the success of the office.

First, the PM–ISE acts as the honest broker in the interagency consideration of the issue, and it operates as the honest broker because it has no turf to defend.

Second, the PM–ISE office is bureaucratically neutral. It has no agency axe to grind, and, in fact, it operates outside of the agency context that, in fact, defines the interagency largely.

And, third, the PM–ISE office has the authority to build the ISE provided it does so by cooperating and coordinating with our Federal, State, local, tribal, and private sector partners. I am called the information manager, and I am indeed the program manager for information. But I am also in large measure the program coordinator. I don't have a budget that can implement the program. I rely on the budgets of the agencies.

I hope that you understand and that the Committee realizes that these characteristics have been essential to the success and they will be essential to the future success of the ISE.

Thank you for the opportunity to speak to the Committee, and I welcome any questions.

Chairman LIEBERMAN. Thank you for that good report, Ambassador.

Next is Charles Allen, Under Secretary for Intelligence and Analysis and Chief Intelligence Officer at the Department of Homeland Security. Thanks again for all your public service, Mr. Allen, and we look forward to your testimony.

TESTIMONY OF CHARLES E. ALLEN,[1] UNDER SECRETARY FOR INTELLIGENCE AND ANALYSIS AND CHIEF INTELLIGENCE OFFICER, U.S. DEPARTMENT OF HOMELAND SECURITY

Mr. ALLEN. Thank you, Chairman Lieberman. It is a pleasure, and "Charlie Allen" is a fine introduction. I don't need anything else.

I really want to commend your Committee for the work that it did in helping create this environment for the sharing of terrorism information through the Intelligence Reform and Terrorism Prevention Act of 2004. And I am pleased to have an opportunity today to talk about what the Department is doing in cooperation with its Federal, State, local, tribal, and private sector partners to ensure that the phrase "information sharing" is not just a buzz word but that it really does reflect action on the part of the Department in helping share information with its principal stakeholders, particularly at the State and local levels. It is a great pleasure to be here to appear with my colleague Ambassador McNamara, with Skip Thomas, with my old friend from the CIA, Jeff Smith, with whom I worked some years ago, and also to have the GAO offering a very good overview of where we are in the area of information sharing.

We at the Department have a statutory mandated role in the Homeland Security Act of 2002, which you had a lot to do with, that is very distinctive in the intelligence community because of our unique set of customers and our focus on the homeland. This role is made even clearer in implementing the recommendations of the 9/11 Commission where the Department was designated as having the lead responsibility for the Federal effort to integrate State and local fusion centers into a National Fusion Center Network to which Ambassador McNamara alluded. And as the Under Secretary for Intelligence and Analysis, I am responsible for implementing those mandates on behalf of the Secretary and the Department, and I want to explain some of the things that we are doing.

Achieving the Department's information-sharing mission requires people and tools, and we have devoted significant resources to providing both of these. Within my office, my team has created the Department's State and Local Fusion Center Program Management Office to build essential relationships with the fusion centers. Through the program office, we have deployed intelligence officers to 25 fusion centers that serve alongside with their State and local partners. We are going to have 10 more intelligence officers deployed by the end of the year, and these men and women serve at the front line for information sharing. They are providing State, local, tribal, and even other Federal partners with the information they need to keep America safe. These same skills permit them to cull the best of what fusion centers are collecting and analyzing and ensure that these data get to the appropriate people in other States, as well as here to the Federal Government.

DHS is committed to providing fusion centers with the information-sharing tools they need to participate in the Information Sharing Environment described by Ambassador McNamara.

[1] The prepared statement of Mr. Allen appears in the Appendix on page 129.

At the Secret level, we have deployed the Homeland Secure Data Network (HSDN). This network is now in 23 fusion centers, and we are working to deploy it to 17 more by the end of the year. Among other things, the network provides access to NCTC On-line classified portal that maintains the most current terrorism-related information at the Secret level. The network also provides the fusion centers with a window into the National Intelligence Community that they can use for their own information needs. Ultimately, every fusion center with this network access will have its own web page where relevant State and local products can be posted and made available to other fusion centers and, of course, to the National Intelligence Community.

At the unclassified level, the Homeland Security Information Network's Intelligence portal provides more than 8,000 people with access to finished intelligence products. To better foster collaboration and share the best practices and lessons learned within the fusion center network, DHS also sponsors the Homeland Security State and Local Intelligence Community of Interest, which we call Homeland Security SLIC. It is a virtual community of intelligence analysts, hundreds of them. Its membership has grown significantly in the past year. We have 43 States participating in SLIC, as well as the District of Columbia, and seven Federal departments. This is a way that intelligence analysts across the country can collaborate via threat conferences, biweekly at the Secret level with secure video teleconferences, and in a virtual community of interest on the Homeland Security Information Network (HSIN) intelligence platform. SLIC also sponsors Secret-level conferences that are annual analytic conferences, and we have at least on annual theme-oriented conference per region.

DHS also is working to ensure that information we share is what our partners need. To do this, we undertook a project with six fusion center partners to examine day-to-day information needs of the fusion centers. As a result, my office was able to develop a set of priority information needs for the fusion centers. We are now seeing joint analytic products serving all levels of the government and the private sector being written by fusion centers in conjunction with DHS and the FBI.

The Department also is providing leadership to important multi-agency organizations dedicated to improving information sharing with our non-Federal partners. An important piece of multi-organizational efforts is the National Fusion Center Coordination Group, a Federal-State partnership that was established as part of the Information Sharing Environment. The Director of my State and Local Fusion Center Program Management Office serves as co-chair of this important group with the Deputy Director of Intelligence at the FBI. The coordination group has had success in fostering the development of fusion centers and bringing them into a cohesive partnership at the State and local level as well as with the Federal partners.

On the content side, Ambassador McNamara talked about the Interagency Threat Assessment and Coordination Group (ITACG), which was established at the direction of the President and implementing recommendations of the 9/11 Commission Act of 2007. This is to facilitate increased sharing of counterterrorism informa-

tion between the National Intelligence Community and with our State and local partners. By pulling together in one place an outstanding group of Federal, State, local, and tribal homeland security, law enforcement, and intelligence officers at the National Counterterrorism Center, there is now a focal point to guide the development and dissemination of Federal counterterrorism intelligence products through DHS and the FBI to our State and partners.

The ITACG achieved Initial Operating Capability on January 30. It is led by one of my senior intelligence officers who serves as its Director. The Deputy Director is a senior analyst from the FBI. Currently, the team includes four law enforcement officers from State and local police departments who work full-time at NCTC. We are working to expand this to at least 10 non-Federal participants from a broad range of expertise, including fire and health departments, homeland security advisers, and other organizations as needed.

The ITACG members have essential systems connectivity in NCTC, participate in key briefings, and are engaged in the NCTC production processes and activities so that they have a broad perspective of the intelligence community, which then they can share information down to the State and local levels.

I chair an Advisory Council of the ITACG on behalf of the Secretary. The council, of which at least 50 percent of the members must represent State, local, and tribal organizations, has become a very robust organization. It includes distinguished Americans, including the Lieutenant Governor of Nebraska. It meets at least four times a year, but I have decided as Chair to meet every month. We either meet face to face or in teleconference. So I am very pleased that the ITACG is truly up and operating effectively.

We are also establishing an attractive Fellowship Program so that we can get the very best from our State and local governments, both law enforcement and non-law enforcement officers to serve in the ITACG. And I am very proud of what we have assembled, both for the detail and for the Advisory Council.

I have only touched on a few areas of where the Department is engaging in information sharing involving its partners at the State and local level. I think we are making real progress. We believe that information sharing is central to our mission. It cannot be an afterthought. The Secretary and I remain committed to implementing the information-sharing mandates of both the Intelligence Reform and Terrorism Act, the Homeland Security Act, and the 9/11 Commission Recommendations Act of 2007. We also work to protect civil rights and civil liberties and privacy, as Ambassador McNamara pointed out.

I look forward to your questions.

Chairman LIEBERMAN. Thanks very much. I was just thinking, as I was listening to you, because you have been involved in intelligence work on our Nation's behalf for quite a while, that you have seen some remarkable changes occur. I take it beyond the written word that you have just given us, this is quite a change from not so long ago in the intelligence community. Am I right?

Mr. ALLEN. You are absolutely right, because I have worked very closely with the National Intelligence Community, being a CIA offi-

cer for some decades, and the lack of information sharing among intelligence community agencies, it may have been a model that worked in the Cold War. We did not make the changes that were required. We did not break down those barriers in the 1990s when we should have. And as a result, this country suffered greatly. We can never afford to do this again, Senator, and I will do everything in my power to ensure that we continue to change and build the culture that Mr. McNamara is trying to build.

Chairman LIEBERMAN. I know you will and you have, and I do not want to jump ahead, but I do think that listening to the testimony—we will go on now—there ought to be reassurance to the American people insofar as they know about what we are up to. And in some sense there ought to be deterrence to our enemies that we have not only raised our guard but broadened it, if I can put it that way.

Mr. ALLEN. At every level, in the private sector, State and local, and at the Federal level, our air, land, and sea borders, it is tough. And we are making it tougher every day.

Chairman LIEBERMAN. Yes. Thanks.

OK. Commissioner Thomas, great to have you here from Connecticut, and I appreciate now hearing from the State perspective about the question at hand.

TESTIMONY OF JAMES M. THOMAS,[1] COMMISSIONER, DEPARTMENT OF EMERGENCY MANAGEMENT AND HOMELAND SECURITY, STATE OF CONNECTICUT

Mr. THOMAS. Thank you very much, Senator Lieberman. Just for the record, my name is James M. Thomas, and I am the Commissioner for the Connecticut Department of Emergency Management and Homeland Security, and I am here to talk to you about the Intelligence Reform Act.

I want to start off to tell you that in my 39 years of law enforcement experience, I have never seen such a strong willingness for people to come together and share information. It was not always like this, and it has taken place as a result of September 11, 2001, I am sure.

We work very closely with the Department of Homeland Security, and they work not only with our State but all the other 50 States. As I am here today, our colleagues are in New York City meeting with New York, New Jersey, and the other New England States on interoperability and information sharing. Monday of this past week, we were in New York City, again, sharing information.

I have participated in and seen the benefit of this collaborative approach, not only in Connecticut but throughout the country. I think DHS has set some standards, guidelines for fusion centers. Everybody is following those standards. That is what we need to do. I think it is very important.

I think that since September 11, 2001, under the leadership of Charlie Allen and Secretary Chertoff, DHS has been a leader providing training, expertise, and analysts to help us get going in this critical mission, and DHS has been successful in preventing future terrorist attacks.

[1] The prepared statement of Mr. Thomas appears in the Appendix on page 145.

I think the key for me—and I came from a local law enforcement agency to the State-level—to terrorism prevention is good, timely intelligence. The motto, which is in our State, should be "Gather, evaluate, analyze, and then share information." That is our motto. Every single piece of paper we put out, we talk about gathering information at the local level, passing it up to the State level, analyzing, and then sharing it. That is what we do 24 hours a day, 7 days a week.

I can tell you that in our part of the country information sharing has never been better. For example, this week, and every week, the Connecticut Intelligence Center weekly bulletin is shared with 169 towns in our State and with tribal nations. It includes information from the local law enforcement, State Police, Department of Corrections, Federal agencies such as FBI, ATF, DEA, TSA, U.S. Coast Guard, and DHS. The Connecticut Intelligence Center weekly bulletin—I brought ours in. It has reports from New York, New Jersey, and the other five New England States.

I think the key thing for us is we can issue these bulletins on an hourly basis, a daily basis, or they always come out every single week. As a former chief of police in two communities, I want to make sure it is hitting the street where the officers need it. I think that is where we are going to make the difference in terrorism-related situations. So when I am out—and I am one of these people who goes out to talk to the police departments, and I want to talk to the officers in the field—I am assured every single day from the patrol officers to chiefs and other command people that they have the information, they are receiving it. They have never seen anything like it in all their careers either.

I think that if we do not do this, this is clearly a big mistake and I appreciate the work you have done, Senator, and that the DHS, FBI, and others have brought into this collaborative effort. There is too much risk if we do not share information with each other. The men and the women out in the field are professionals. They are on the front line. They deserve the very best means of preventing or stopping a terrorist incident from happening.

I think the key for us is, again, it must be done at the local level. That is where the information is. In our State, we ask every organized police department to put an intelligence liason officer (ILO) program in place. We at the State level put five regional intelligence officers (RILOs) out. Our five regions in the State of Connecticut touch base every single day with the ILOs. That is where the information comes in. We gather it, we analyze it, we disseminate it. I think the ILO/RILO program we have in our State is really what makes our State unique, and it is really working well.

In our Intelligence Center, we have local officers, State officers, Federal officers. You would not know who they are and what agency they are from. We also have analysts primarily from FBI, Homeland Security, TSA, Coast Guard, and the governor has authorized us to hire a State analyst also.

I think it is really important that we also engage the private sector, and, again, really through the Department of Homeland Security, Mr. Allen's office in particular, we have an analyst in the State of Connecticut. She provides us with what we call "open source documentation," stuff that is out there that is non-classified,

but very important information, and it is given to us at a State level, a regional level, national, international. We take this information. which is open source. We put it on our secure portal. We make it available to people on our State portal with the private sector.

As a result of engaging the private sector, we are getting information from them on a daily basis. We have a very effective Suspicious Activity Report (SAR) program, in Connecticut. We think it models what they are doing in Los Angeles, but we are always looking for change, and we are looking for the best possible practice.

In conclusion, times have changed. The threat of terrorism-related activities is real and a constant concern. So the way we do business needed to change. This change is now taking place. I believe and hope that your Committee will continue to support and fund the fusion centers that have been developed and will support our goal of having well-trained intelligence analysts from the Federal, State, and local agencies working side by side analyzing the information and intelligence that they receive and, most importantly, disseminating it back to the street where it needs to be shared.

This past March, the Department of Homeland Security and the Department of Justice sponsored a National Fusion Center Conference. All 50 States, territories, and possessions were there. Highly interactive. I was there. And I could tell you, working together, we can and will make a difference. We need to work together like we have never done it before, and if we work together, I honestly believe the United States will be a safer place.

I see the first responders—the local and the State officers—as first preventers. They are the ones who are going to make the decisions out in the field. And our State and I think a lot of States are also doing that through the mobile data terminals. An officer in the field, through their little computer in the car, has access to our intelligence briefing—again, hourly, daily, and weekly. Information is really at their fingertips, and we are very pleased for that.

Again, thank you very much for the opportunity to speak to you today, Senator. I am proud of what we are doing in Connecticut, but, more importantly, I am proud of what we are doing on a regional basis and the national level under your leadership.

Chairman LIEBERMAN. Thanks very much, Commissioner. I am grateful for what you are doing in Connecticut and beyond.

Just while I think about it, say a little bit more about the involvement of the private sector because that is, obviously, critical in terms of the control of critical infrastructure but more generally. Are they self-motivating in this area?

Mr. THOMAS. Yes, I think we realize that, just from a security viewpoint, you take any urban area in the State of Connecticut and 85 percent of the assets are owned by the private sector. They need and support the Federal Government and State government. They want to be engaged. They even have their own security forces that sometimes outnumber the local law enforcement by 10-fold. In a city like Hartford or New Haven, they may be lucky if there are 70, 80 officers in the field. There are thousands of private security. If we can engage them, they know what is happening, and they see

suspicious activity. If they trust us and we have a relationship with them, which I think is critical, they will report suspicious activity. That is where it is. We think that working with the private sector is a smart thing to do. We are doing it in Connecticut. We have had many conferences with them. They want to be engaged with us, and we are doing that.

Chairman LIEBERMAN. Great. Thanks very much.

Our final witness on the panel is Jeffrey Smith, a partner at Arnold and Porter, previously with the Central Intelligence Agency, a real expert in this field. Thanks for being here, Jeff. I look forward to your testimony.

TESTIMONY OF JEFFREY H. SMITH,[1] PARTNER, ARNOLD AND PORTER

Mr. SMITH. Thank you, Mr. Chairman. It is a pleasure to be here and to appear on this panel and to thank the Committee in person for the efforts that you have done over the years.

I have been asked to appear this morning because of my service on the Markle Foundation Task Force, and under the leadership of Zoe Baird and former Netscape CEO Jim Barksdale, the Markle Foundation convened a bipartisan task force, of which I am a member, to examine national security in the information age.

Let me emphasize at the beginning that I am appearing here today on my own behalf, not on behalf of the task force, although I have consulted with several members of it.

This diverse group met with government officials, private industry, experts on technology and civil liberties, and foreign partners in order to find solutions for this critical information-sharing problem. We issued a series of reports and advocated the creation of a trusted information-sharing environment that ensures the twin goals of national security and civil liberties. I am pleased that the government has taken many of our recommendations to heart, and this Committee deserves special recognition for the role it has played.

As the GAO found in its report released today, the Information Sharing Environment has improved dramatically. The Congress, the President, and the intelligence community have made much progress, although much still needs to be done. Significant cultural, institutional, and technological obstacles remain. There is reason to be concerned that the initial focus and momentum have dissipated a little bit, while confidence in the process and deliverables has decreased. I don't mean to be the only one speaking negatively, but we are picking up some of this, I think, despite the really extraordinary efforts of Ambassador McNamara, Charlie Allen, and others. One cannot allow the recent reforms or the absence of a new attack on our homeland to lull us into complacency.

It is true, as you say, Mr. Chairman, the Nation is certainly safer, but our enemies get smart as well, and we need to stay one step ahead of them.

As our task force recommended, this effective information-sharing environment must be built on trust. The agencies must trust

[1] The prepared statement of Mr. Smith with an attachment appears in the Appendix on page 149.

each other with sensitive information. The American people must trust their government to protect their civil liberties and privacy. Realization of this trust environment urgently requires sustained leadership and strong oversight from all branches of government; clear policies, processes, and guidelines; and technologies that facilitate sharing while protecting privacy and security.

The Markle Task Force will continue to assess the government's progress, and we are currently preparing a report card that will make what we hope to be constructive recommendations to give to the next President and to Congress that will help the Nation move forward in its information-sharing system.

Let me touch on a few issues. I have a longer prepared statement, Mr. Chairman, but let me just touch on a few of these.

Congressional leadership is needed to proactively exercise oversight responsibilities and provide adequate funding for the implementation of information-sharing provisions. There is a lot of new legislation that has passed, but I also urge the Congress to stay on top of this. I also worry a little bit about the overlapping jurisdiction of some of the oversight and appropriations committees, which is always a difficult issue up here. As the Chairman will remember, I was General Counsel of the Armed Services Committee for a while, and I am very familiar with these issues. I know it is difficult, but I hope the Congress will take a hard look at these issues.

Presidential leadership is also necessary to steer implementation across agencies, facilitate the kind of cultural transformation that is required, and encourage public confidence in the government's information-sharing policies. The White House has recently issued a comprehensive information-sharing strategy, standardized the classification system, and streamlined the security clearance process. All good moves.

Earlier this year, Ambassador McNamara released his second Annual Report to Congress. I commend you for your work and that of your colleagues. The Executive Branch efforts have initiated a paradigm shift from a "need to know" to a "need to share" culture.

I also welcome the GAO's report and Charlie Allen's effort. However, the Administration must ensure that transforming the government in order to improve information sharing and collaboration is an urgent priority that does not wane or fall victim to turf battles and ambiguity about responsibility and authority.

Finally, leadership is needed at the State and local level to improve coordination, standardize information-sharing procedures, and evaluate progress. I am impressed by what Commissioner Thomas just reported to us, that there has been a lot of progress. Again, we continue to hear occasional problems at the fusion centers that have their roots not in bad intentions, but in inadequate sharing of information and a certain amount of turf warfare that is inevitable in any organization.

Let me talk about two or three of the most important policy recommendations of the Markle Task Force. I have listed others in my statement, but let me touch on just a couple.

First, a core recommendation of the Markle Task Force is the adoption of an authorized use standard. Under such a standard, agencies or employees could obtain mission-based or threat-based permission to access or share information, as opposed to the cur-

rent system which relies on place-of-collection rules, U.S. Person status, or originator control—ORCON—limitations. The Administration has looked at this and said that they thought adopting that would be difficult because of privacy guidelines. I am confident that if we work hard, an authorized use standard is achievable.

Also, let me touch briefly on an issue of enormous importance to all of us—the protection of privacy and our civil liberties. The ISE has issued guidelines that require that information sharing complies with the Constitution. Each agency now needs to develop its own guidelines consistent with the ISE's.

As this Committee knows, the law also established the Privacy and Civil Liberties Oversight Board, and that functioned briefly. However, after its first report in 2007, one of its members resigned because he believed that the board interpreted its responsibilities too narrowly and lacked sufficient independence from the White House. In response, Congress wisely reconstituted the board as an independent agency within the Executive Branch. By statute, the board should have been up and running by January 30 of this year. It is regrettable that a full slate of new board members has neither been nominated nor confirmed. And the Congress and the President should breathe new life into this important institution, if not this year, surely in the new Administration.

We also have called for greater training and development of human capital. We have talked about measures to improve decisionmaking by officials. The Director of National Intelligence (DNI) has done a great job in focusing on greater use of open source information. The success of the mission managers for hard targets like North Korea and others have proven to be a big success. I think they go a long way, but we still have a ways to go.

I also believe that we need to focus on vertical integration of State, local, and private actors. The Interagency Threat Assessment and Coordination Group has begun to support the NCTC by sharing Federally coordinated information with others. That is important.

Finally, the status of technology. We believe in the Markle Task Force that there is some technology that can be extremely valuable to achieving this goal of improving our security and protecting civil liberties. These include the use of immutable audit logs and anonymizing information technology. Again, the Administration has looked at these and said that they are not convinced that the technology exists. Well, let me state that differently. They believe it exists, but have reservations about the expenses associated with trying to adopt it and the good results that could be achieved. Our view in the task force is that this technology is there, can be adapted, and we urge the Administration and Congress to consider funding this technology.

Mr. Chairman, I look forward to your questions. The Markle Task Force will continue its work with Congress. It looks forward to working with the transition team for the new President, and as I said earlier, we hope to make some recommendations to the new Administration. We do this on a bipartisan basis. This is far too important for any partisan issues to creep in. That has been the way our task force has worked. That is the way this Committee has worked. And we look forward to working with you.

Chairman LIEBERMAN. Thanks, Mr. Smith. Very helpful.

Incidentally, the Markle Task Force has followed the lead of the 9/11 Commission in that your members have stayed active and continue to monitor progress in this area. It is very important.

Take a minute and just tell us a little more about a word that we do not see in use much here on Capitol Hill. It is called "anonymization." I guess I had a double meaning in my reference, but now I mean a singular meaning. Tell us about anonymization technology.

Mr. SMITH. Anonymization technology is technology that permits information to be shared without identifying the person about whom the information describes. In other words, in the current rules, based on old technology, we have a series of minimization procedures in which if we acquire information that has the name of an American citizen, that is stricken and that name can be disclosed with proper authorization.

Anonymization would permit looking across much broader pieces of data banks, data information, and looking at that information to detect patterns, but at the same time not identifying to the user the names of the American citizens who might be in that data bank. And it is very sophisticated technology that we believe would permit the government to do some of the things it needs to do without impinging on the privacy of American citizens.

Chairman LIEBERMAN. Understood. Charlie Allen, do you have a reaction to that? Is that something we should be investing in?

Mr. ALLEN. Well, I think we have to look at all such tools because, as you know, part of our issue has been how to lawfully and appropriately use information on U.S. persons. And I agree with the Markle Foundation recommendations ought to be fully examined as a tool to do this.

The main thing we have to do is what I do, that all my officers, including myself, take every year very rigorous review of how to handle U.S. information. There has to be reasonable belief before us to use that type of information. We just do not use any information on U.S. persons. It has to be used with great rigor and great oversight from our Legal Department.

Chairman LIEBERMAN. Let me ask this question, and I suppose appropriately it should be to Charlie Allen, Ambassador McNamara, and Commissioner Thomas. You have given us some encouraging reports as to the progress we have made on information sharing since September 11, 2001. I wonder, within the bounds, obviously, of either—this is another form of anonymization, as I think about it—not disclosing classified information or discussing cases that have become public in some way, whether you can put a little flesh and bone on this. In other words can you bring to mind any specific situations where the new information-sharing environment has actually helped you to connect the dots in a way that allows you to take action you would not otherwise take? Obviously I do not need names here if they are not public. Do you have any that comes to mind, Mr. Allen?

Mr. ALLEN. I think absolutely where we had some arrests in South Carolina last year—first responders, as Skip Thomas pointed out, were very vital. That information we immediately put at the Federal level, involved the State of Florida.

Chairman LIEBERMAN. So it came from first responders?

Mr. ALLEN. Absolutely, and I was called on a Saturday night, and I activated my officers in both South Carolina and in Florida, and we had a lot of information that I could immediately brief the Secretary on.

So the information-sharing examples—we just recently had one over the 3rd and 4th of July. It was a minor incident that turned out to be a criminal event back in the Northeast. But initially it was—it did give us some alarm, but working with State and local officials, who were very open, we were able to run traces and checks and found out it was a criminal action and had nothing to do with terrorism at the time. But it did give us concerns initially, and I remember talking to the Secretary even about the issue.

So we have had incidents here, incidents in California where Chief Bratton and others have called upon the Federal Government, NCTC, and ourselves to quickly supply information, as well as the Bureau. It is a whole new culture. It is learning to collaborate and work together in ways that are absolutely unprecedented.

Chairman LIEBERMAN. So in the South Carolina case, did local first responders apprehend someone or see something suspicious?

Mr. ALLEN. They stopped a car that was speeding, and then because of the suspicious behavior of the occupants, they then detained the individuals, and as a result of that, without getting into the particulars, it is clear that it became an FBI investigation case.

Chairman LIEBERMAN. Excellent. Commissioner, do you have any examples?

Mr. THOMAS. Yes. I think what Mr. Allen had indicated to you is a prime example I believe. It is going to be an officer in the field, a trooper in any one of the 50 States who can make a routine stop, run a name through the computer, and if there is cause—and that is what happened in South Carolina, and as a result, information was developed. And I have seen it just on a practical basis. That is why in Connecticut we do an all-crimes approach. We do everything from—you name it—murder, rape, robbery, or assault. That bulletin hits the streets. It is full of photos of suspects, actual crimes that have occurred. And I will tell you, within hours sometimes many cases are solved. Others lead to other situations.

Chairman LIEBERMAN. Because you are running them through other databases.

Mr. THOMAS. Correct. And, it crosses State lines, and it is amazing. It is a tremendous source of information. It is effective, and people really trust each other. And when the people in the field know that they are being heard and they have credibility, they are really likely to give you more information.

Chairman LIEBERMAN. Ambassador, do you have any examples?

Mr. MCNAMARA. I think the best example I can give is a pilot program that we ran with the FBI, my office and the FBI, in which we actually took the information from the databases, and we were able to move it to a controlled environment that allowed BlackBerry access to it by law enforcement officers on the street in New York and Washington, DC. In doing this, we found that they were able to pinpoint much more accurately exactly who it was they were looking for, who they would find. They were able to look at

photographs, for example, on their BlackBerry while the individual that they were working on was present within eyesight.

The BlackBerry project was so successful that the FBI in the end has funded this BlackBerry program for every FBI agent and all the Joint Terrorism Task forces (JTTFs) around the country. And we hope to see it extended to all the local law enforcement officers that work with the JTTFs.

In practical terms, that pilot program was underway in New York at the time of the JFK tank farm case. And it played a role in that particular case.

Chairman LIEBERMAN. That is great.

My time is up. I will say that by coincidence you have before you the two Members of the Senate who may be most BlackBerry addicted. [Laughter.]

We are constantly competing, Senator Pryor and I, to see who has the latest version. Perhaps the program that you have described, Ambassador, could be extended to the Senators.

Mr. MCNAMARA. I will see about that, Senator.

Chairman LIEBERMAN. All right. Senator Pryor, thanks for being here.

OPENING STATEMENT OF SENATOR PRYOR

Senator PRYOR. The Chairman always has a nicer BlackBerry than me. It causes a lot of consternation on my part. I am always a step behind him.

Let me start with you, Mr. Allen, and follow up on something you said in your statement. You mentioned that the Department of Homeland Security is establishing a fellowship to allow State and local fusion center analysts to serve on the Information Sharing Coordination Group. Can you tell us a little bit more about that and what the timetable on that is?

Mr. ALLEN. Yes, and this has been a very energized effort on our part because we and the FBI, working under the management of the National Counterterrorism Center, are establishing this Interagency Threat and Coordination Group. The FBI had an established program for bringing officers in from the State and local level. This is something new to the Department of Homeland Security. So we have worked very hard—my office and my information managers, working with the ITACG and the Advisory Council of the ITACG. We have established a program where now we have the same kind of incentives and benefits essentially that the FBI has in bringing people from State and local law enforcement officers, homeland security specialists, or health specialists into this ITACG. And it has worked out very well because they have to have a place to stay here, they have to have some funds to travel home on a relatively reasonable basis. They have to have a vehicle in order to get around the Washington area. And they have to have something that, when they finish their tour of duty here, which right now is for a year at a time, that they can go back to their own police departments, and this will be a boost to their career. Being away from a police department does not help unless you have something to really show for it when you go back. We are going to train really outstanding people who know all-source intel-

ligence, working with all this sensitive information, and are able then to help sanitize a lot of it and get it down to State and local.

This experiment, I think, as Ambassador McNamara said, is proving to be a very successful, good beginning. We have only been in business about 6 months, but we are making progress.

Senator PRYOR. And how many do you think will be in the fellowship at any given time?

Mr. ALLEN. We hope to have up to 10 people at any given time, and then rotate them in and out on a staggered basis, the individuals serving a year at a time.

Senator PRYOR. Mr. Allen, let me ask if the DHS strategy with respect to supporting State fusion centers, and sometimes the Federal Government and the State government have a different view of things. Do you feel like that your strategy in trying to support State fusion centers has the same objectives and goals that they do at the State level?

Mr. ALLEN. I think we have the same goals because we deal primarily, obviously, against the terrorism threat, but we also support, as Mr. Thomas said, all threats to our homeland, which is a little broader. So I think our goals are the same. What we have to do, of course, is to learn—and in my written statement, I talk about how we have run a pilot program with six of the fusion centers to make sure we understand fully the needs and requirements and the priorities of State and local. Because at the Federal level, we provide intelligence obviously that may not be as relevant or as useful at the State and local level.

We have learned a lot over the last couple years, so I think we have identified the priorities and needs, at least in a measured sense at the State and local level, but we have a lot to learn, and we are very sensitive to the need to listen rather than to transmit from the Federal Government.

Senator PRYOR. And do you see fusion centers playing a long-term role with the Department of Homeland Security?

Mr. ALLEN. I think they are going to play a role for years and decades to come, knitting together in what we call this National Fusion Center Network and working horizontally with other fusion centers across the country. They are naturally sort of grouping into various sectors, like the Southeast, the Southwest, and the Northeast. And as they work vertically up to the Federal level, I think we are going to see a richer exchange of information, and also I think we are going to see a safer country, because we are going to be able to hopefully detect and disrupt activities that are nefarious and designed to hurt this country.

Senator PRYOR. A minute ago, we talked about the Fellowship Program that you are establishing right now. Let me ask a question on the training that analysts go through. Is it important that analysts have a consistent training across the country? Or should that training be more individualized on the State level?

Mr. ALLEN. I think it is important that we at the Federal level take the lead because we have been working on intelligence training and analytic trade craft for decades. Obviously, it has to be changed and modified for the State and local intelligence officer, intelligence analyst, but we are doing this.

Right now, with the help of the Director of National Intelligence, we are developing a State and local intelligence course, which we will have ready by the 1st of October, that is really directed at the official use level where we can teach. Meanwhile, we are sending mobile teams out to train intelligence analysts, and also I am bringing officers in as part of my intelligence training program to train my own analysts because I have a lot of analysts that need training.

This is very essential. If we are going to be successful, the Federal Government has got to work with the State and local to help train those analysts and train them in what we have learned over many decades as a result of our experience in the Cold War and beyond. The context, the information, and how we do analysis are different. But the principles remain the same, and the Federal Government has to work very hard with State and local government. And I am committed to this, Mike Leiter at the NCTC is, I know Mr. McNamara is, and I know the DNI is committed to help us train analysts at the State level and local level.

Senator PRYOR. And a question we always get from our State and local people is who pays for that training.

Mr. ALLEN. Well, that is a bit issue, and that is one that the Secretary is in a better position to answer. I do know that the Secretary has extended working with OMB. We extended for a third year intelligence analytic training, and so there is an additional year that has come about as a result of the Secretary's work with the Office of Management and Budget.

I believe at a certain level, the Federal Government has to be involved because we have the—we work very hard with the schools. There is a CIA University. There is a National Intelligence University. The Defense Department teaches over in the Defense Military Intelligence College. There are a lot of tools, techniques, and ways that we should be helping the State and local governments, and we need to impart that information.

Senator PRYOR. Thank you, Mr. Chairman.

Chairman LIEBERMAN. Thanks, Senator Pryor. I appreciate your being here.

Notwithstanding all the improvement that we have made—and it really is quite significant, nonetheless, as I indicated earlier, GAO continues to put information sharing on the high-risk list. And I wanted to ask you, Ms. Larence, if you would just say a little bit about why and what you are looking for to be able to have GAO remove this from the list. In other words, what are the parameters of it, first? Is it information sharing generally? Is it related to homeland security? What is missing?

Ms. LARENCE. It is more specifically related to terrorism information sharing as opposed to the homeland security emergency response information sharing. And what GAO looks for in making the decision whether to take something off of the list is: Do we have a clear, organized, and structured plan in place; do we have the resources and the commitment in place; and do we have a good way to measure progress.

So we do not wait to ensure that all the I's are dotted or all the T's crossed, but if that infrastructure is in place and we can dem-

onstrate that it is, then we entertain taking those issues off the list.

We have been working collaboratively with the Ambassador's office and the Office of Management and Budget on what the plan is for coming off of the list, what commitments they would make to the plan, and what it would take to get off the list. And we have been monitoring that progress every 6 months.

Chairman LIEBERMAN. Right. So let me now ask you, Ambassador, and perhaps Mr. Allen, how you understand the placement on the high-risk list and what you are doing to try to get off it.

Mr. MCNAMARA. Well, it may sound somewhat paradoxical, but I welcome the fact that information sharing is on the high-risk list because I think it is a matter that demands constant attention and a priority position, and things on the high-risk list tend to get that attention and get that priority. That is also the reason why I welcome the GAO report. It is a fresh set of eyes looking at a very complex problem and giving us insights into where we need to do better.

We all welcome the pat on the back when we do well, but it is also good to have somebody looking over our shoulders to try to help us to do even better.

I think that the way to get off the high-risk list is to institutionalize and routinize the Information Sharing Environment. Since we have not yet gotten to the point where the Information Sharing Environment is fully functional, that is the first thing we have to do. And by making it fully functional, I mean, as I said in my opening remarks, that it becomes part of the ordinary way in which government does business. That has not happened yet, and it is not surprising that in a few years—this huge bureaucracy and the complex government structure we have, this Federal structure goes out to the State and local and tribal areas, and, indeed, there is even the cooperation to a more limited extent with our allies and partners overseas—it has not become routinized in the way in which we hope to have it.

So I think that by placing the priority on it—and here I do disagree with GAO. There is a road map. The initial road map was the implementation plan, as I said in my opening remarks. That has been refined by the President's National Strategy for Information Sharing. Nobody can doubt what the priority areas are and what the road ahead is as seen by the Administration, writ large. So we are probably a little behind—and here I agree with GAO's critique. We are behind in, if you will, the metrics of how we measure the progress we have made, but I think there is no doubt that we have made a significant amount of progress. And, indeed, making the progress, in my book, took precedence over measuring whatever progress we made.

Chairman LIEBERMAN. Yes.

Mr. MCNAMARA. And I think that the way we are going to get off the high-risk list—and I do not think we should come off the high-risk list until there has been a determination made by the Administration, by the Congress, and by those of us working on this, that we have institutionalized a fully functioning Information Sharing Environment. And that is some years in the future.

Chairman LIEBERMAN. Mr. Allen.

Mr. ALLEN. Mr. Chairman, I agree with my colleague. I like to have oversight, and I like to have the pressures. And if GAO and you all view our information-sharing work today as high risk, I would agree because we are in the very early stages of this. We are breaking barriers month after month, and as you can see, just forming the ITACG, just building connectivity, both unclassified and secure, getting our officers deployed, starting to speak the same language at the State and local level takes time. With the accesses that we now have, some of the information we have is very sensitive, and we have to strip out the information from the sources and methods.

We know how to do this. In the past, we have been reluctant to really work at that problem. Now we understand how to do it. The security rules are changing. This controlled and classified environment, controlled unclassified info (CUI), that we are now working on here with Ambassador McNamara is going to help a great deal. But it is going to take a while to institutionalize this. We are just in the early stages, and we are just in the early stages of working and training analysts at the State and local level and to intelligence analytic trade craft. But we are going in the right direction, and we just need to now push a lot harder in the next several years.

Chairman LIEBERMAN. Interesting. So really you are saying flat out that this is not something we should want to see come off the high-risk list next year. If it does, you would say it would be unjustified because of the tremendous change in the status quo that is necessary, but also because of the consequences.

Mr. ALLEN. I think that, as Ambassador McNamara said, has to be a decision made by the Administration and by the Congress, and it has to be evaluated.

Chairman LIEBERMAN. Right.

Mr. ALLEN. And he is right. Using metrics, we still are working hard to determine their progress. We know we have made progress, and we see visible results on a daily basis. But we need a more structured, organized, institutionalized way of operating our Information Sharing Environment.

Chairman LIEBERMAN. Ms. Larence, do you want to say anything in response to what the Ambassador and Mr. Allen have said?

Ms. LARENCE. No, sir. It sounds good to us.

Chairman LIEBERMAN. OK. Ambassador McNamara.

Mr. MCNAMARA. Could I add a couple of points with respect to how we measure this?

Chairman LIEBERMAN. Sure.

Mr. MCNAMARA. When I came into this job a little over 2 years ago, what I was hearing—to use the phrase very frequently used here on the Hill—from my constituents or my customers at the State and local level was, "It is broken. We are not getting the information." What I am hearing now, and what you have heard here in this hearing from non-government officials, is that, "It is not fully fixed, but it is an awful lot better than it was before."

I take that as a metric. I go out, my staff goes out to dozens of conferences. We have visited dozens of fusion centers. We have talked with hundreds and hundreds of first responders, homeland security officials, law enforcement officials, and government offi-

cials at the State and local level, and they are all saying, "It is much better." That is a metric. I am not sure GAO could quantify it, but I take that constituency response as being a metric.

One other point. I said at the beginning of my statement that we had no model on which to build this ISE. We looked around and there was nothing in government that we could model on. I take it as a compliment and as an indication of progress and of success that, in the last several months, three other efforts to create Information Sharing Environments within the government have come to us to try and learn from what we have done. I am sure you and the Committee are aware of the FAA's next-generation air transport system.

Chairman LIEBERMAN. Right.

Mr. MCNAMARA. The FAA has come to our office to learn about the technologies, the architecture, and the standards that we have set up so that they can adapt and apply them for their air transport system. The Maritime Domain Awareness Network that is being set up by the Department of Defense, the intelligence community, the Department of Transportation, and others is looking to try to integrate the information flows within the maritime environment, both military and commercial. That means ports, transport, etc. They came to us to study our progress over the course of the last couple of years to see how much of that they could take and apply to their upcoming information environment.

And, finally, the Department of Health and Human Services is sponsoring a nationwide Health Information Network that they hope to have up and running. They also came to us to try and take our templates, if you will, and apply them.

So I think we are moving along at a pretty good clip.

Chairman LIEBERMAN. I would say you should take that as a compliment. That is great.

Let me move to this question of the authorized use standard, which the Markle Task Force recommended, which would replace the current system of place-of-collection rules and originator control with mission-based and threat-based permissions to access and share information.

The 9/11 Commission Act required the ISE to report to Congress on the feasibility of an authorized use standard, and we did, in fact, receive that report in March. The ISE noted that such a standard would be difficult to implement under existing law and would potentially contravene privacy- and civil liberties-related laws and executive orders.

I wanted to ask you first, Ambassador McNamara, given these objections, one, whether you believe that the move to the authorized use standard is a good idea; and, two, how you believe the legal framework would need to be altered to permit that standard to go into effect.

Mr. MCNAMARA. I think in principle, an authorized use standard is a very valuable tool that would assist in establishing a fully functional Information Sharing Environment, a fully functioning ISE. There are, in fact, regulatory and legal rules that prevent us from moving directly to an authorized use standard in the short term. But I think we—and by that I mean the program manager's office and the major agencies involved in this—and that is the De-

partment of Justice, the Office of the Director of National Intelligence, the Homeland Security Department, and the Department of Defense—have, in fact, underway studies to see how one can move to that.

I think in all likelihood—and I am not an expert in this area by any means—that we are going to move to that by stages rather than just one fell swoop. For example, I think it will be easier to move to authorized use within an agency structure than it will be to move multiple agencies at the same time to an authorized use standard.

Chairman LIEBERMAN. Mr. Smith—I am sorry, Ambassador. Do you want to go further?

Mr. MCNAMARA. One last thing, and that is that we need to define authorized use, and then we are going to have to come back to the Congress and change laws and regulations that right now operate on a different standard.

Chairman LIEBERMAN. Thanks.

Mr. Smith, why don't you talk a bit about what definition of authorized use you would like to see, and then comment on the ISE's report and the necessary legal changes to implement this idea.

Mr. SMITH. The notion of an authorized use standard is to sort of turn things around. To make sure we all understand it, in the current rules, the purpose for which information is disseminated is determined by the person who collects it. It is driven by a series of rules, like if it is a U.S. person and information, it follows certain channels.

The idea was that we ought to have, instead of these rules that are based on the manner in which it was collected, it ought to be disseminated for the purpose for which it can be used. And in that sense, it is kind of turning things on its head.

In the Markle Task Force, we anticipated some of these problems. I will be frank with you. I think we thought it would be a little easier than it has proven to be. But we certainly respect what the Administration has done. I am pleased that Ambassador McNamara's report, that they are looking hard at it.

I don't know, Mr. Chairman, as I sit here this morning, that I have specific suggestions as to what laws might need to be changed or whether regulations need to be changed. But to the extent they do need to be changed, I think they are worth looking very closely at because we do think that this can go a long way.

In my mind—and I would be interested in the reaction of my colleagues—it is not unlike what the intelligence community is doing on the front end; that is to say, with the mission managers, where they have a more effective way of trying to coordinate targeting of intelligence collection. And this would in a sense, then, be the other end of that telescope where the information is then disseminated for the authorized use of that information rather than necessarily basing it on whether it is SIGINT, HUMINT, COMINT, or something else, which then puts it into a particular channel that determines its dissemination.

Chairman LIEBERMAN. Good enough. Mr. Allen, do you have a reaction to this discussion?

Mr. ALLEN. I simply affirm essentially what both Jeff Smith and Ted McNamara have said. It is going to take time. It is going to

be incremental. We obviously have to change because the rule set today I think is too rigid about those who originate and collect the information. But under the current policies and probably certainly from a legal perspective, there will have to be significant change over time to implement an authorized use standard. I think we have to work toward that. I believe that Jeff Smith is right. But I think like Ambassador McNamara, it is going to take time. But we should work at this goal because in the past it has inhibited the full flow and sharing of information. In our Department, it took us 18 months to ensure that we can share information just across all segments of this Department, which is 210,000 people. You would think you could have done that in a month. It took 18 months.

Chairman LIEBERMAN. Understood.

Commissioner, let me go to you on the fusion centers. These have been really a significant forward development to facilitate information sharing among Federal, State, and local agencies. Let me just ask you the open-ended question acknowledging that you have testified that they have made real progress, they have been helpful. Is there anything further that you would like to see or that you need from the Federal Government to assist you at the State level in your mission here?

Mr. THOMAS. I think the key thing for us, Senator, is the long-term sustainability of these fusion centers. I think we have started making great progress, and I see it at the local level, I see it at the State level, and the cooperation we have been receiving from the Federal level—whether it be from DHS, FBI, Coast Guard, or others I could name—has been tremendous. But for us this is going to have to be a long-term investment.

Coming from the local side, I cannot expect the Federal Government to pay 100 percent of it. We are paying a lot of personnel—it's a big commitment—but we have to do this for many decades. And I think it is critical that we have a portion of the homeland security—some of the advisers have even said, OK, let's take a percentage of any homeland security grant we get. The most important thing for us today, I think, is going to be information sharing. The days of buying equipment and training, those are good, but you need information.

So the most important thing we can look for is going to be long-term sustainability of these intelligence/fusion centers. That to me is going to be the key.

Chairman LIEBERMAN. Ambassador McNamara.

Mr. MCNAMARA. Yes, I fully agree. I think what we are doing here is we are going through a period of adjustment as a new phenomenon or, if you will, a new set of institutions comes onto the horizon, and that is fusion centers.

I want to stress that, at least from my perspective, it is very important to see the fusion centers in terms of all crimes, all hazards, not just terrorism, because I think they are not sustainable around the country if they only do terrorism. There are a few places where that will work. New York City is an example, L.A. and probably Washington, DC, where you would get a very high volume of terrorism work and information that needs to be worked on. But for the country at large, I think they need to be all crimes, all hazards. That means we have to look at the funding with a much broader

perspective than just homeland security, just terrorism, or just even law enforcement in many cases.

I think we need to look at this so that these fusion centers evolve and develop into valuable commodities for the localities in which they are in; that is to say, the States and the major urban areas. And if that is the case, then they will get funding from the States and the major urban areas because it is worth it to those governments and those localities to fund it. And the Federal Government will get information coming from those State and local fusion centers that will be valuable to the Federal Government, not just in terrorism but in other areas.

If we can look at it with this more holistic approach, I think we can work out the details of who funds what and what share of the cost ought to be borne by what element of our federated governmental structure.

Mr. ALLEN. I would just like to add——

Chairman LIEBERMAN. Go ahead.

Mr. ALLEN. Mr. Chairman, I agree with that, this broader all-threat, because in homeland security intelligence, we look at terrorism, but we look at it through the prism of homeland security intelligence, which includes secure borders, because bulk cash couriers could be carrying money for drug-trafficking organizations, or they could be carrying money for Hezbollah. So trying to narrowly separate out terrorism from these broader threats does not help. I think representing the fusion centers as all-threat, all-hazard is the right way to go, and I believe Ambassador McNamara has the essence of the issue here, that there are broader reasons than just terrorism why these fusion centers are going to be very valuable—smuggling networks, other proliferation, loss of U.S. technology. There are a lot of reasons why State and local fusion centers are needed and needed for the foreseeable future.

Chairman LIEBERMAN. Yes, absolutely. You all make a strong point, and obviously modern information technology enables that kind of sharing and networking to occur, not only more easily but more instantaneously than before. So this is a new age we have entered.

Secretary Allen, let me ask you about a particular case which shows both the value of information sharing, but then some of the privacy challenges that we have. I know the Department of Homeland Security has been working with the National Counterterrorism Center to find a way to provide access to information in the arrival and departure information system run by the US-VISIT program in a way that appropriately cross-checks that database against known terrorism information, but is also consistent with privacy laws and standards, for example, by promptly disposing of records where there is not a match.

Can you talk to us about that, about some of the challenges associated with that kind of activity. Very important to do, of course, for our homeland security, and yet we want to be careful about the information we gather. How is that going?

Mr. ALLEN. I think it is going well. Still, as Secretary Chertoff, were he here, would say, there is progress to be made. We are very good on air and sea entries into this country. We very carefully ensure that the names of individuals are checked against the Ter-

rorist Screening Center, which is run by the FBI, to ensure that they are not on any lists that would indicate any type of nefarious activity. And that works well. It is rare that anyone—extremely rare that anyone gets past that particular check.

We also are working hard, as you know, with the Western Hemisphere Travel Initiative, to have identity cards, and so that we will avoid the kind of problems that some people have because even though they have nothing to do with another individual of the same name or similar dates of birth, that is something we are working very hard on. The watchlist, as it has been reported in the press, is being refined, and where you have only the last names or the first names, those kinds of data are being eliminated from the watchlist so that we have a more streamlined and more effective way of tracking people as they come into this country and they are not held up when they are traveling.

A problem, of course, is on the outgoing to ensure—we do not have at this time complete systems for exit determining who has left the country.

Chairman LIEBERMAN. Right.

Mr. ALLEN. And that is going to be—that is a huge challenge. It is going to take a lot more study and a lot of technology, and it is obviously going to take a lot of resources to do that.

But I think overall—and I know that the Secretary has given this high attention because he was speaking about this earlier this morning.

Chairman LIEBERMAN. Excellent. Thanks.

Another question that is about incentives within the Department. The 9/11 Commission Act of 2007 included a section that gave agencies the authority to consider, "the success of an employee in appropriately sharing information," and that should be considered when making determinations on monetary incentives and cash awards to Federal employees.

I wonder if you have any report on what progress is being made to implement this provision to provide incentives to employees to effectively promote and engage in information sharing, either Ambassador or Secretary.

Mr. ALLEN. I would just say that my intelligence organization is moving to pay for performance in accordance with what the Director of National Intelligence desires. That is obviously one of the criteria that will be used in evaluating employees as to their performance, and we are looking for ways to innovate, and some of the innovation that we have developed within the Department on new systems of connectivity—I talked about the State and local community of interest, the fact that we can link now to 43 States and the District of Columbia where endless talk weekly, either at a classified level or official use level, is unprecedented. And we are awarding people who are involved in this kind of innovative thinking within the Department.

Chairman LIEBERMAN. Ambassador, do you have a response?

Mr. MCNAMARA. Yes. In fact, one of the metrics that we have set up is to measure the incentives and disincentives to information sharing in the agencies that are members of the Information Sharing Council. There are 17 of them.

We are finding the responses from the agency are that information-sharing incentives a year ago were about 40 percent, and they grew to about 73 percent, according to the reports from the agencies. What we are now doing, having gotten in that data, is we are going back and through the summer, spring, and fall of this year examining exactly what those incentives are. But we know of many of them, and others we are looking very closely at.

One of them, for example, is the one that Charlie Allen alluded to, and that is, the Director of National Intelligence, Mike McConnell—who, by the way, is an absolutely committed and very strongly committed individual with respect to information sharing—has mandated that within the intelligence community that there be in all employee reports an aspect of the employee's evaluation report which covers that employee's performance with respect to sharing information. We know, for example, that the FBI has an awards program for sharing information, and other agencies are also coming in.

We are also interested in reducing disincentives, that is, to reduce the number of rules and regulations that are being applied within an agency that restrict information flows, and obviously originator controlled (ORCON) information is one of those. But reducing the ORCON and other restrictions generally tends to be done agency by agency, and what we are looking to do is to set up—and we have not gotten to it yet—a set of guidelines for incentives and disincentives to information sharing that we can get a general agreement on throughout the interagency, and then issue the guidelines with instructions that agencies should implement the guidelines and include the incentives and disincentives in their programs.

We are also working with the Office of Personnel Management, OPM, to see whether or not OPM can help us with these incentives and disincentives.

Chairman LIEBERMAN. That is excellent.

Two more questions from me. One is the fusion center guidelines that were published jointly by DHS and DOJ suggested that there was a role for non-traditional sources of intelligence, from the not so non-traditional as the fire service to, for instance, private sector. And, Secretary Allen, let me start with you. I wonder if you think there is a value to the fire service and other non-traditional entities being involved in the Information Sharing Environment, and if so, particularly through the fusion centers, what is happening in that regard from your perspective.

Mr. ALLEN. I would believe that non-traditional sources of information are important—the fire departments and public health service are going to be important as we look at controlling pandemics perhaps or getting early warning of pandemics. We are developing a relationship with fire departments across the country, with the New York City Fire Department, I have a very close relationship, and we have provided information, equipment, and classified capabilities to the New York Fire Department, as we do to the New York City Police Department.

So it is going to be important that we find non-traditional information. We think that, still respecting private sector, civil rights, and civil liberties, non-traditional intelligence sources are going to

be vital to us in the coming months. When we had the terrible accident in New York City, the Corey Lidle, the small plane that hit an apartment building, it was the fire department that was there first to help deal with that problem.

Information from fire departments is going to be very important to us in the future, and I know that probably Skip Thomas would support that view.

Chairman LIEBERMAN. Yes, that is good to hear. I was going to ask you, Skip, what your response is.

Mr. THOMAS. I think it is very critical——

Chairman LIEBERMAN. Are they involved with you now at all?

Mr. THOMAS. Yes, to some degree, and what we think—the fire marshal's office, which is extremely critical regarding any major investigation, plus the fire service is just a tremendous source of information out there. They deal with all kinds of hazardous material. They have access to every facility that is in any city, town, or county in the United States. I think they are extremely critical of that. Again, that trust relationship has got to be there. There are tremendous men and women in that service.

It is the same thing with public health. We had a very difficult case in Connecticut, if you remember, the anthrax case, and the first people on the scene were EMS, fire service, public health officials, and we worked with their laboratories. So we have to reach out to everybody and to still respect the rights of everybody that is impacted. But the Fire Service and public health are really tremendous sources. That is why we think even in the private sector—in our State, we have an Infoguard chapter with our FBI. It is very strong, about 800 members in it. And we continue to meet, at least on a quarterly basis, and again, it is true collaboration at its very best.

Chairman LIEBERMAN. Good.

Ambassador, let me ask you the last question about the desire of some people, apparently, in the budget bureaucracy—in OMB to defund and disband your office, presumably by fiscal year 2010. I presume you think that is a bad idea. I hope you do. And I just wonder if you could give us a response to the reality of that threat and how you respond to it.

Mr. MCNAMARA. Well, as you know, Senator, we are funded through 2009, and the decision of OMB was that they were not going to put into their current cycle of budget figures new initiatives that were not already in there. It turned out that our office has been funded by the ODNI out of hide; that is to say, the ODNI has given us the funding without actually stipulating in the budget that it was to be funded.

Chairman LIEBERMAN. You mean for 2009 or——

Mr. MCNAMARA. Before 2009—or since we started operating.

Chairman LIEBERMAN. Oh, I see what you are saying, right.

Mr. MCNAMARA. So it did not show up, and according to the OMB regulation, if you will, or rule for this cycle, since it is the end of the Administration, it did not show up and, therefore, I guess technically they are defunding it for fiscal year 2010. But I think that is something that the new Administration is going to have to look at when they come in.

Chairman LIEBERMAN. So did you think it was not substantive but procedural?

Mr. MCNAMARA. I think it started as being a technical aspect of this cycle of the budget call for data, the budget data call that OMB was putting out. You will have to ask them. They have not told me. I have not been consulted on this. I have not been asked for my opinion, and I am prepared to talk about it on the proper occasion as this transition period comes upon us.

Chairman LIEBERMAN. Got it. In any case, of course, it will be relevant for the new Administration making a recommendation for the 2010 fiscal year.

Mr. MCNAMARA. Yes. I think, to give you my personal opinion, that the Office of the Program Manager has been an engine for change in this area. We have not done all the change, but we have been the engine driving the change. And the fact is that we have a 3-year implementation plan out there. As the GAO has noted, we have not finished with that. There is work still to be done. I have not heard anybody say that we have done what needs to be done in this area.

I think it is up to the President and the Congress to decide on the future of this office. It was intended to be temporary. The original mandate was for 2 years. I think people recognized immediately the complexity of the problem made the 2-year limitation almost laughable. And, therefore, both the Congress and the President, jointly and separately, have extended it indefinitely.

I think it is up to the President and the Congress, therefore—the Congress originally launched the idea of the Information Sharing Environment, and this Administration has supported it strongly.

Chairman LIEBERMAN. Right.

Mr. MCNAMARA. And, therefore, I am ready to discuss and put my 2 cents in, if you will. I plan myself personally to be leaving. I came out of retirement, as I said to someone a couple of weeks ago, I came here to build the foundation, not to complete the building. And I intend to move on. But I think the question of the office is important and needs to be discussed, and I think we have to make a distinction between the office and the functions. The office may be and indeed is temporary. But the functions that are being developed and being carried out by this office are going to be around for a long time.

For example, the CUI that we have, we built the framework for the CUI. The President endorsed it and instructed agency heads to go out and implement the CUI regime. Rather than maintain the control of the CUI regime in our office, we passed it off to the National Archives and Records Administration (NARA), a permanent entity but an entity like us that has no bureaucratic turf to defend and no agency stake in it. They—NARA—will run the CUI regime indefinitely into the future. Somebody has got to—once we get the SAR program up and running fully, somebody other than the PM–ISE Office is going to have to take that on in order that the program be continued indefinitely into the future. And so much of what we are doing, the function remains even when the office disappears.

Chairman LIEBERMAN. Well, first, you are right that Congress intended the office to be temporary, and I think that is still the intention. I hope we come to a point where, as you have said, the office is not necessary. But it is very clear that we have not reached that point yet, so I think there will be a lot of opposition, beyond my own, to defunding or disbanding the office, if that is a decision that the next Administration makes. I also want to thank you for taking this role, and I think you should feel some pride yourself that you built a strong foundation for whoever follows to build the building.

I want to thank all of you for your testimony today. To me, this is a very encouraging hearing, notwithstanding the constant necessity to try to get as close to perfection as we can because of the consequences of imperfection here. But there has been really a remarkable transformation in information sharing among the different levels of government and within the Federal Government. And I cannot thank you enough for what you have all done to bring that about. If I may modify a familiar phrase, your persistent vigilance is, in fact, the price of the safety and liberty of the American people, and I thank you for it. And this Committee will continue to do whatever we can to both monitor and oversee your progress, to pester you occasionally, but most of all, to try to support you in the critical work that you do.

We are going to leave the record of the hearing open for 15 days if any of you want to submit any additional comments for the record or if any of my fellow Committee Members who could not be here this morning want to submit questions to you. But in the meantime, I cannot thank you enough, really, for what you do, not just in testifying today but what you do every day for our country.

Thank you very much. The hearing is adjourned.

[Whereupon, at 11:55 a.m., the Committee was adjourned.]

APPENDIX

PREPARED STATEMENT OF SENATOR VOINOVICH

Mr. Chairman and Ranking Member Collins, I commend you both for convening today's hearing to discuss information sharing among Federal, State, and local governments.

The importance of sharing law enforcement and homeland security information became apparent after the events of September 11, 2001. In recent years, dozens of information sharing fusion centers have been created across the country to streamline intelligence gathering and share information among Federal, State, and local officials.

My home State of Ohio has such a fusion center that is experiencing success with its information sharing efforts. The center is working with more than two dozen Federal, State, and local agencies as well as the private sector, and that work has allowed interested parties to write important and useful reports that have been used for a variety of purposes. In fact, Ohio's fusion center was one of six State centers that were recently recognized for outstanding performance at the National Fusion Center Conference.

Information sharing is allowing for important national security work like that being conducted at the Ohio fusion center. However, there are unresolved questions and areas of concern as Federal, State, and local law enforcement work to share information.

First, the potential use of private sector data by fusion centers has led to questions about privacy and civil liberties violations. We must ensure that as law enforcement officials collect and share intelligence, they afford appropriate protections to personal information and appropriate deference to individuals' right to privacy. At the National Fusion Center Conference, Ohio was recognized for its privacy protection policies and practices. I hope Ohio's work and efforts can serve as a useful guide for other information collecting and sharing efforts.

Second, as the Chairman knows, Senator Akaka and I have worked for years to bring a performance-based approach to how the government manages access to sensitive national security information. Included in these efforts are our work to lessen the amount of time it takes to investigate and adjudicate security clearance applications as well as our efforts to ensure that Federal agencies recognize security clearances granted by other Federal agencies. To my dismay, I understand State and local officials have had difficulties obtaining security clearances in a timely manner for individuals who need access to classified information and also problems getting Federal agencies to recognize security clearance granted to State and local officials by other Federal agencies. We have got to find a way to address these problems, and I hope today's hearing discusses some potential solutions.

Again, I want to thank the Chair and Ranking Member for calling today's hearing, and I appreciate the witnesses spending some time with the Committee today to discuss this matter. Sharing information in a smart way can greatly help us secure our Nation.

United States Government Accountability Office

GAO

Testimony

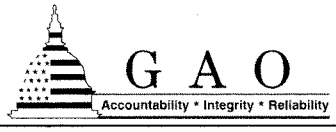
Before the Committee on Homeland Security and Governmental Affairs, U.S. Senate

For Release on Delivery
Expected at 10:00 a.m. EDT
Wednesday, July 23, 2008

INFORMATION SHARING

Definition of the Results to Be Achieved in Terrorism-Related Information Sharing Is Needed to Guide Implementation and Assess Progress

Statement of Eileen R. Larence, Director,
Homeland Security and Justice Issues



GAO-08-637T

July 23, 2008

GAO
Accountability·Integrity·Reliability

Highlights

Highlights of GAO-08-637T, a testimony before the Committee on Homeland Security and Governmental Affairs, U.S. Senate

INFORMATION SHARING

Definition of the Results to Be Achieved in Terrorism-Related Information Sharing Is Needed to Guide Implementation and Assess Progress

Why GAO Did This Study

In 2005, GAO placed the issue of information sharing for homeland security on its high-risk list of federal functions needing broad-based transformation and since then has monitored the government's progress in resolving barriers to sharing. This testimony discusses three key information sharing efforts: (1) the actions that have been taken to guide the design and implementation of the Information Sharing Environment (ISE) and to report on its progress, (2) the characteristics of state and local fusion centers and the extent to which federal efforts are helping to address some of the challenges centers reported, and (3) the progress made in developing streamlined policies and procedures for designating, marking, safeguarding, and disseminating sensitive but unclassified information. This testimony is based on GAO's products issued from March 2006 through July 2008 and selected updates conducted in July 2008.

What GAO Recommends

GAO is recommending that the ISE Program Manager more fully define the ISE's scope, results to be achieved, and stakeholders' roles and responsibilities, including the development of performance measures and defining the federal government's long-term role in relation to fusion centers, including the provision of resources. The ISE Program Manager generally agreed with these recommendations.

To view the full product, including the scope and methodology, click on GAO-08-637T. For more information, contact Eileen Larence at (202) 512-6777 or laurencee@gao.gov.

What GAO Found

In a report being released today, GAO concludes that the ISE, under the leadership of a designated Program Manager, has had a measure of success, but lacks a road map for guiding the ISE, ensuring accountability, and assessing progress. The Program Manager's Office issued an implementation plan in November 2006 to guide the design of the ISE, has carried out a number of steps in that plan, and has leveraged existing efforts and resources agencies independently pursued for improving information sharing. However, this plan lacks important elements essential to effectively implement the ISE. Gaps exist in (1) defining the ISE's scope, such as determining all the terrorism-related information that should be part of the ISE; (2) clearly communicating and distinguishing the role of the Program Manager and other stakeholders; and (3) determining the results to be achieved by the ISE (that is, how information sharing is improved) along with associated milestones, performance measures, and the individual projects. Two annual reports on progress have been issued. Each identifies annual goals and individual ISE efforts, but neither reports on the extent to which the ISE has improved information sharing.

GAO reported in October 2007 that fusion centers, established by states and localities to collaborate with federal agencies to improve information sharing, vary widely but face similar challenges—especially related to funding and sustaining operations—that the federal government is helping to address but are not yet resolved. While the centers varied in their level of maturity, capability, and characteristics, most fusion centers focused on processing information on crimes and hazards, as well as terrorism-related information. Fusion center officials reported facing challenges such as obtaining specific, clear guidance and training; obtaining and retaining qualified personnel; and securing funding for center operations over the long term. The Department of Homeland Security and the Federal Bureau of Investigation were helping to address these challenges by, for example, providing technical assistance and training, personnel, and grant funding. Also, legislation has been proposed to clarify how funding may be used to hire and retain intelligence analysts.

Although the myriad of sensitive but unclassified designations has been a long-standing problem, progress has been made in establishing processes for designating, marking, safeguarding, and disseminating this information. In March 2006, GAO reported that each federal agency determined sometimes inconsistent designations to apply to its sensitive but unclassified information and this could lead to challenges in information sharing, such as confusion on how to protect the information. Thus, GAO recommended that the Directors of National Intelligence and the Office of Management and Budget issue a policy that consolidates sensitive but unclassified designations. In a May 2008 memorandum, the President adopted "controlled unclassified information" (CUI) to be the single categorical designation for sensitive but unclassified information throughout the executive branch and provided a framework for designating, marking, safeguarding, and disseminating CUI.

Mr. Chairman and Members of the Committee:

Thank you for the opportunity to summarize the results of our recent reviews of the government's efforts to better share information about possible terrorist threats to protect the homeland. As you know, in 2005, GAO placed the issue of information sharing for homeland security on its high-risk list of federal programs or functions needing broad-based transformation and since then has conducted work to monitor the government's progress in resolving barriers to sharing. What we found is that in the wake of 9/11 and the passage of the Intelligence Reform and Terrorism Prevention Act of 2004 (Intelligence Reform Act) and Implementing Recommendations of the 9/11 Commission Act of 2007 (9/11 Commission Act), agencies at the federal, state, and local levels are taking steps to better share information about possible terrorist threats.[1] New organizations whose mission is information sharing and fusion have been created. New processes, information systems, and networks have evolved to handle the sharing and to encourage communication among the partners who must analyze and act on this information. And Congress and the administration have enacted new laws and issued new policies, guidance, and standards to promote better sharing. But there is still important and critical work left to do. This includes better integrating all of these changes and initiatives into a set of functioning policies, processes, and procedures for sharing; continuing to break down agency stovepipes and cultures that promoted protection over sharing; monitoring and measuring progress; and maintaining momentum.

Among the many efforts begun to improve information sharing is the creation of the Information Sharing Environment (ISE), a governmentwide "approach that facilitates the sharing of terrorism and homeland security information, which may include any method determined necessary and appropriate."[2] In implementing this initiative, the Program Manager for the ISE—appointed by the President and responsible for planning, overseeing, and managing this new approach with participation of other federal departments and agencies, such as the Departments of Defense, Justice, and Homeland Security—envisions an ISE that will be comprised of policies, procedures, and technologies that link people, systems, and

[1]See Pub. L. No. 110-53, 121 Stat. 266 (2007); Pub. L. No. 108-458, 118 Stat. 3638 (2004). See also Pub. L. No. 107-296, 116 Stat. 2135 (2002).

[2]See Pub. L. No. 108-458, § 1016, 118 Stat. at 3664-70, amended by Pub. L. No. 110-53 § 504, 121 Stat. at 313-17.

information among all critical stakeholders. In addition, most states and some local areas have created fusion centers to address gaps in homeland security and law enforcement information sharing by the federal government and to provide a conduit for this information within each state. While they vary—reflecting differences in state and local needs—a fusion center is generally a "collaborative effort of two or more federal, state, local, or tribal government agencies that combines resources, expertise, or information with the goal of maximizing the ability of such agencies to detect, prevent, investigate, apprehend, and respond to criminal or terrorist activity." One of the barriers to information sharing with these entities was the many different and sometimes confusing and contradictory ways that agencies were identifying and protecting sensitive but unclassified information. This information encompasses a large but unquantifiable amount of information—for example, sensitive law enforcement information, information about a narcotics-smuggling ring, and terrorism financing information—that does not meet the standards established by executive order for classified national security information, but that an agency nonetheless considers sufficiently sensitive to warrant restricted dissemination.

My testimony today summarizes the findings of our work on the following three information sharing initiatives: (1) the actions that have been taken to guide the design and implementation of the ISE and to report on its progress, (2) the characteristics of state and local fusion centers and the extent to which federal efforts are helping to address some of the challenges centers reported, and (3) the progress made in developing streamlined policies and procedures for designating, marking, safeguarding, and disseminating sensitive but unclassified information. The information in this testimony is based on GAO reports and testimonies issued from March 2006 through June 2008 addressing these three

terrorism-related information sharing issues.[3] We also conducted selected updates in July 2008 by obtaining and reviewing the *Annual Report to the Congress on the Information Sharing Environment*, dated June 30, 2008, released after our report on the ISE was issued, and the May 2008 *Memorandum for the Heads of Executive Departments and Agencies: Designation and Sharing Controlled Unclassified Information*, released since our work on that issue. We conducted this work according to generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Summary

In a report we are releasing today, we conclude that one of the primary ways in which Congress and the administration intended to promote sharing—through the ISE under the leadership of a designated Program Manager—has had a measure of success, but lacks a road map that defines the scope of the ISE, roles and responsibilities and the desired results to be achieved (i.e., how information sharing should be improved), and measures for assessing progress. The Program Manager's Office issued an implementation plan in November 2006 to guide the design of the ISE, has achieved a number of steps in that plan, has incorporated into the ISE a number of initiatives that agencies independently pursued to leverage resources, and has issued two annual reports on its progress. However, this progress is tempered by several gaps to be filled, such as:

- The Program Manger and participating agencies have not yet fully defined the scope of the ISE—or what the ISE is and is not to include—

[3]See GAO, *Information Sharing Environment: Definition of the Results to Be Achieved in Improving Terrorism-Related Information Sharing Is Needed to Guide Implementation and Assess Progress*, GAO-08-492 (Washington, D.C.: June 25, 2008); *Homeland Security: Federal Efforts Are Helping to Alleviate Some Challenges Encountered by State and Local Information Fusion Centers*, GAO-08-35 (Washington, D.C.: Oct. 30, 2007); *Homeland Security: Federal Efforts Are Helping to Address Some Challenges Faced by State and Local Fusion Centers*, GAO-08-636T (Washington, D.C.: Apr. 17, 2008); *Transportation Security Administration's Processes for Designating and Releasing Sensitive Security Information*, GAO-08-232R (Washington, D.C.: Nov. 30, 2007); and *Information Sharing: The Federal Government Needs to Establish Policies and Processes for Sharing Terrorism-Related and Sensitive but Unclassified Information*, GAO-06-385 (Washington, D.C.:
Mar. 17, 2006).

and completely answered fundamental questions, such as what information should be shared, where does the information reside, and what systems and networks will be integrated into the ISE. Addressing these gaps is important and necessary to establish a clear road map to guide implementation for all entities involved, ensure that progress is made based on needs, and facilitate future measurement of progress in information sharing.

- The role and responsibilities of the Program Manager versus those of the key agencies involved were not clearly distinguished and communicated, slowing progress. Delineating clear roles and responsibilities will minimize confusion over what each stakeholder is accountable for in implementing and operating the ISE and help minimize unnecessary delays that result.

- The Program Manager and stakeholders have yet to fully define the results to be achieved and milestones, performance measures, and individual projects for assessing progress. Linking measurable long-term and interim goals and clearly defining measurable results to be achieved can help the Program Manager and stakeholders track progress of implementation and improved sharing as well as hold stakeholders accountable for meeting their responsibilities and contributions in ensuring the ISE's success.

The ISE and information sharing for protecting the homeland against terrorism is a complex and ever-evolving challenge. Addressing these gaps, while difficult, is nevertheless necessary to provide Congress and the public reassurance that the flaws leading to 9/11 have been or are being corrected. Therefore, to address these gaps and help ensure that the ISE is on a measurable track to success, we recommended that the Program Manager, with full participation of relevant stakeholders (e.g., agencies and departments on the ISE), (1) more fully define the scope and specific results to be achieved by the ISE along with the key milestones and individual projects or initiatives needed to achieve these results, and (2) develop a set of performance measures that show the extent to which the ISE has been implemented and sharing has been improved—including, at a minimum, what has been and remains to be accomplished—so as to more effectively account for and communicate progress and results. The Program Manager generally agreed with these recommendations. The recently issued 2008 annual report comes closer to addressing these gaps, but acknowledges that work remains to be done to move from measuring

individual agency actions and progress to measuring the overall performance of the ISE and the results and outcomes achieved.[4] But our work shows that there are still important questions for the administration and Congress to answer: Does the federal government know where it is going and what it is trying to achieve in the end? How far has it come and how much is left to do? Is this progress good enough? How much better is the sharing and what difference has it made? What will it cost? Finding these answers will be challenging but critical for ensuring homeland security.

With respect to our work on information fusion centers, we reported in October 2007 that these centers vary widely and that a number of them face several similar challenges—especially related to funding and sustaining operations—that the federal government is helping to address but that are not yet resolved. More specifically, our work showed that states and localities generally created these centers to improve information sharing across levels of government and to prevent terrorism or other threats. At the time of our review, the centers varied in level of maturity and capability, but most focused on processing information related to crimes or hazards, not just terrorism-related information. As we reported, most were led by law enforcement entities; had a variety of partnerships with other federal, state, and local agencies; and had federal personnel assigned. Among the challenges fusion center officials reported that they faced were managing a high volume of information from multiple systems, obtaining specific and clear guidance and training on operational issues, obtaining and retaining qualified personnel, and securing federal grant or state and local funding for center operations over the long term. We reported in October 2007 that the Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI) were helping to address these challenges by, among other things, providing access to information systems and networks as well as technical assistance and training, deploying personnel to centers, and providing grant funding. However, to improve efforts to create a national network of fusion centers as envisioned for the ISE, we recommended that the federal government determine and articulate its long-term fusion center role and whether it expects to provide resources to centers to help ensure their sustainability. To some extent, the administration did so in the *National Strategy for Information Sharing: Success and Challenges in Improving Terrorism-*

[4]Program Manager, Information Sharing Environment, *Annual Report to the Congress on the Information Sharing Environment* (Washington, D.C.: June 30, 2008).

Related Information, issued in October 2007, by stating that the federal government will support the establishment of fusion centers and help sustain them. The 9/11 Commission Act further reflects this and legislation has been proposed to clarify how Homeland Security Grant Program funding may be used to hire and retain intelligence analysts.

Finally, as to the barriers to sharing posed by agency practices in protecting sensitive information, we found that although the myriad of sensitive but unclassified designations has been a long-standing problem, a recently issued policy should help to streamline and standardize the process for designating, marking, safeguarding, and disseminating this information. In March 2006, we reported that U.S. government agencies had varying and disparate designations—such as law enforcement sensitive, for official use only, and unclassified controlled nuclear information—for identifying sensitive but unclassified information. At that time, there were no governmentwide policies or procedures that described the basis on which agencies should designate, mark, and handle this type of unclassified information, resulting in each agency deciding how to do this on its own. We reported that such inconsistency could lead to challenges in information sharing, such as confusing those receiving the information—including local and state law enforcement agencies—who in turn must understand and safeguard the information according to each federal agency's rules. Consequently, we recommended the issuance of a policy that consolidates sensitive but unclassified designations where possible and addresses their consistent application across agencies, as well as a directive requiring that agencies have in place internal controls for the designation and use of this information. To address this concern and in line with our recommendations, in a May 2008 memorandum, the President adopted "controlled unclassified information" (CUI) to be the single categorical designation for sensitive but unclassified information throughout the executive branch; outlined a framework for identifying, marking, safeguarding, and disseminating this information; and made the National Archives and Records Administration (NARA) responsible, through its new CUI Office, for implementation and oversight. While the new policy is a good start, our work has demonstrated that monitoring agencies' compliance to ensure that they implement guidelines, training, and internal controls will help ensure that the policy is employed consistently across the federal government. The Transportation Security Administration's (TSA) program on managing information it designates as sensitive security information could serve as a model to guide other agencies' implementation of CUI. We found that the program institutes many of these key components, such as employee training on how to decide what information to designate as sensitive security information,

and internal controls, such as supervisory review to ensure that employees are appropriately making these designations.

Stakeholders Are Taking Steps to Improve Terrorism-Related Information Sharing, but Existing Gaps Present Challenges for Implementing the ISE and Measuring Its Progress

ISE stakeholders are taking steps to improve terrorism-related information sharing, but work remains to define the scope of the ISE, roles and responsibilities, the desired results to be achieved—that is, how information sharing should be improved—and measures for assessing progress, all elements in establishing a road map for meeting information sharing needs and implementing the ISE. For example, because these gaps, such as the need to better define roles and responsibilities, have not been fully addressed, additional effort has been spent reinforcing that all stakeholders are accountable for defining the ISE, not just the Program Manager. For example, in response to the Intelligence Reform Act, the President appointed a Program Manager for the ISE and on December 16, 2005, issued a memorandum to implement guiding principles—the presidential guidelines—consistent with establishing and supporting the ISE.[5] In addition, an Information Sharing Council (ISC), chaired by the Program Manager and currently composed of 16 other members—including designees of the Departments of State, Justice, and Homeland Security—has been established to provide interagency support and advice to the Program Manager on the development of the ISE. A step in planning for the ISE and putting it into operation included the issuance of the *Information Sharing Environment Implementation Plan* in November 2006. This plan provides an initial structure and approach for designing and implementing the ISE and addresses ways to meet the ISE requirements set forth in the Intelligence Reform Act as well as the presidential guidelines. For example:

- The plan includes steps toward standardizing procedures for protecting information privacy. One such activity identified in the plan includes having the Program Manager and key stakeholders establish a process for ensuring that nonfederal organizations participating in the ISE implement appropriate policies and procedures for providing protections.

- The plan maps out a timeline for further defining what information, processes, and technologies are to be included in the ISE and exploring

[5]See Presidential Memorandum, *Memorandum from the President for the Heads of Executive Departments and Agencies, Subject: Guidelines and Requirements in Support of the Information Sharing Environment* (ISE) (Dec. 16, 2005).

approaches for implementing these processes and technologies. The plan consists of a two-phased approach for implementing the ISE by June 2009. Phase 1, originally scheduled to be completed by June 2007, generally covers setup activities such as investigating existing or emerging search technologies for use in the ISE, and relationship building among stakeholders through participation on the ISC. Phase 2, that was to commence in July 2007, covers design as well as implementation of the ISE. The two phases are comprised of 89 total action items organized by priority areas, such as improved terrorism information handling. While 48 action items were to be completed by June 2007, by the end of Phase 1, only 18 were completed. Completed activities include development of proposed common terrorism information sharing standards—a set of standard operating procedures intended to govern how information is to be acquired, accessed, shared, and used within the ISE—and implementation of electronic directory services pages to help identify sources where terrorism information may be located within the federal government and whom to contact to access it.

- Design and implementation also incorporate independent initiatives that federal, state, and local agencies had under way to enhance information sharing across the government. This is in accordance with the Intelligence Reform Act's call to build upon existing systems capabilities in use across the government. These initiatives include the fusion centers state and local governments created and plans to develop a national network of these centers to improve sharing among federal, state, and local entities. They also include the FBI's Terrorist Screening Center, which consolidates information on known or suspected terrorists who operate within the United States for dissemination to federal agencies that use the information to screen individuals for possible terrorist links.

The plan also includes several gaps, however, which have tempered progress in implementing the ISE. Components needed to remediate these gaps include more fully defining the scope of the ISE, clarifying stakeholder roles and responsibilities (i.e., that of the Program Manager as distinguished from those of the departments and agencies that own and must share terrorism-related information), and defining the results to be achieved by the ISE as well as the associated milestones, performance measures, and projects needed for effective program planning and performance measurement. These are all important elements for establishing a road map for and ensuring stakeholders are held accountable in meeting information sharing needs, implementing the ISE, and measuring progress.

To expand on each of these three points, first, the Program Manager and the federal agencies that are key to making the ISE work—such as the Departments of Defense, Homeland Security, Justice, and State—still have work to do to define the scope of the ISE, or what is and is not to be included in it. For instance, the Program Manager and stakeholders are still addressing fundamental questions, such as what information should be shared, where the information resides, how the information will be shared yet protected, how to provide access to information yet respect privacy, and what systems and networks will be used as part of the ISE. We recognize that the ISE will evolve over time and that these questions will need to be revisited and the answers updated and incorporated into the ISE. Answering these questions, at least for the near term, is important and necessary because it helps determine the elements critical for conveying what the ISE is to include and identifying available stakeholder resources—all components needed to establish a clear road map to successfully implement the ISE.

Second, the implementation plan did not clearly communicate and distinguish the role and responsibilities of the Program Manager from those of the key agencies in implementing the ISE and improving information sharing. This has ultimately led to confusion over what each stakeholder will be held accountable for in implementing and operating the ISE. In describing the role of the Program Manager, officials at the Office of the Program Manager noted that his role is primarily as a facilitator and, for example, one who focuses on improving existing business processes or remaining barriers that affect information sharing among two or more of the five ISE communities[6] that make up the ISE. However, the Program Manager does not focus on processes that are internal to ISE members unless they directly impact the wider ISE. Agencies, on the other hand, are accountable for identifying and sharing the terrorism information they own if the ISE is to succeed. However, at the time of our review agencies reported that they were unclear about the Program Manager's role or what their agencies were to provide in support of the ISE. Meanwhile, program officials reported that agencies were not participating consistently and effectively. As a result, this conflict has slowed progress in implementing the ISE, as evidenced by the fact that 30 of 48 Phase 1 implementing action items remained incomplete at the end

[6]As described in the ISE implementation plan, the ISE is comprised of five "communities of interest," encompassing intelligence, law enforcement, defense, homeland security, and foreign affairs. Each community may comprise multiple federal organizations and other stakeholders; information is to be shared across these communities.

of the phase in June 2007. To address these concerns, the President in October 2007 released the *National Strategy for Information Sharing*[7] that reaffirmed that stakeholders at all levels of government, the private sector, and foreign allies play a role in the ISE and further defined the role of the Program Manager as also assisting in the development of ISE standards and practices. However, the strategy did not further clarify the parameters of the Program Manager's role and what is within the scope of his responsibilities in "managing" the ISE versus other ISE stakeholders. In November 2007, the Program Manager held a first-time, off-site meeting with ISC members to focus on ISE priorities, clarify responsibilities, and emphasize the importance of everyone's active participation and leadership—with the intent of rectifying any misperceptions and reinforcing that all ISE stakeholders are responsible for the ISE. Further delineating clear roles and responsibilities will minimize confusion over what each stakeholder is accountable for in implementing and operating the ISE and help minimize unnecessary delays that result.

Finally, work also remains in further defining the results to be achieved by the ISE, the projects needed for implementing the ISE, and the milestones to be attained—all important elements for effective program planning and performance measurement. Existing federal guidance as well as our work and the work of others indicates that programs should have overarching strategic goals that state the program's aim or purpose, that define how it will be carried out over a period of time, are outcome oriented, and that are expressed so that progress in achieving the goals can be tracked and measured.[8] Moreover, these longer-term strategic goals should be supported by interim performance goals (e.g., annual performance goals) that are also measurable, define the results to be achieved within specified time frames, and provide for a way to track annual and overall progress (e.g., through measures and metrics). Following these practices can help the Program Manager and stakeholders track progress and hold stakeholders accountable for meeting their responsibilities and contributions in ensuring the ISE's success. The Program Manager and

[7]The White House, *National Strategy For Information Sharing: Successes and Challenges in Improving Terrorism-Related Information Sharing* (Washington, D.C.: Oct. 31, 2007).

[8]See, for example, GAO, *Results-Oriented Government: GPRA Has Established a Solid Foundation for Achieving Greater Results*, GAO-04-38 (Washington, D.C.: Mar. 10, 2004); GAO, *Executive Guide: Effectively Implementing the Government Performance and Results Act*, GAO/GGD-96-118 (Washington, D.C.: June 1996); Office of Management and Budget, Circular A-11, *Preparation, Submission, and Execution of the Budget* (July 2007); and The Project Management Institute, *The Standard for Program Management*© (2006).

stakeholders have taken action in accordance with these program management principles, but gaps remain. For example, the implementation plan identifies six longer-term strategic ISE goals. For example, one of these goals is that to the maximum extent possible, the ISE is to function in a decentralized, distributed, and coordinated manner. However, the plan does not define what this goal means or set up interim or annual goals and associated time-sensitive milestones to be built upon to achieve the overall goal. Furthermore, the plan does not define how agencies will measure and ensure progress in meeting the strategic goal in the interim or overall. Instead, the plan notes that performance measures will be developed at a later date. Moreover, with regard to identifying the steps to be taken in implementing the ISE, the plan does not present the projects and the sequence in which they need to be implemented to achieve this strategic goal in the near term or in the future, or the specific resources needed and stakeholder responsibilities. Therefore, work remains in developing the road map for achieving this strategic goal.

Since the issuance of the implementation plan, the Program Manager and participating agencies have taken steps to assess progress and improve the ISE's road map by issuing two annual reports and defining annual goals and performance measures, in part consistent with federal guidance for program planning and performance measurement. But taken together, these efforts do not yet provide methods to hold agencies accountable for ensuring that the necessary sharing of terrorism information is under way and effective. More specifically, the first annual report issued by the Program Manager in September 2007 describes overall progress by citing advancements in implementing individual initiatives that contribute to the ISE. Some of these were accomplished under the implementation plan—such as the formation of the electronic directory services—and others were achieved prior to or separate from efforts to create the ISE—such as the establishment of the FBI's Terrorist Screening Center. However, the report does not show how much measurable progress has been made toward implementing the ISE, how much remains to be done, or a road map for completion. For example, the only means to track progress that was set up in the implementation plan was the two-phased approach and the 89 action items. But the progress report did not provide an accounting of the status of these action items or identify how much of the implementation had been completed. Moreover, while the 2007 annual report identifies four performance goals for 2008, information necessary for assessing progress in meeting these goals—such as a defined starting point or baseline against which to assess progress, targets to be reached, or supporting performance measures and interim milestones to be achieved in implementing the ISE—is not identified.

In the fall of 2007 the Program Manger, with input from ISE participating agencies, developed performance measures in support of the four performance goals identified in the annual report. These measures are intended to improve reporting on progress in implementing the ISE and represent an important first step in providing quantitative data for assessing progress made in information sharing and in helping to inform Congress and other stakeholders of specific information sharing improvements. However, there are several gaps in these measures. For instance, they focus on counting activities accomplished rather than results achieved to show the extent to which ISE strategic goals and implementation have been attained. The performance measures include, for example, the number of ISE organizations with a procedure in place for acquiring and processing reports on suspicious activities potentially related to terrorism, but not how the reports are used and what difference they are making in sharing to help prevent terrorist attacks. Similarly, the measures attempt to assess the creation of a culture of sharing by tabulating the percentage of relevant ISE organizations that have an information sharing governance body or process in place, but not by measuring the outcome—such as how and to what extent cultural change is being achieved. Taking the next step—from counting activities to measuring results or outcomes—will be difficult, particularly since the program is still being designed, but critical for accurately providing Congress and policymakers with the information they need to assess the amount and rate of progress, remaining gaps, and the need for any intervening strategies.

Though issued after we completed our June 2008 report,[9] we subsequently reviewed the second ISE annual report dated June 30, 2008 and determined that the Program Manager has taken steps to improve assessments of progress in the ISE as program officials noted they would during our review. However, gaps still remain in defining key aspects of a road map—such as its scope, roles and responsibilities, and results to be achieved. One improvement, for instance, is that the Program Manager tried to better align agency activities according to the five guidelines and two requirements presented by the President in his 2005 memorandum[10] rather than listing them independently. For example, toward addressing

[9]GAO-08-492.

[10]See Presidential Memorandum, *Memorandum from the President for the Heads of Executive Departments and Agencies, Subject: Guidelines and Requirements in Support of the Information Sharing Environment (ISE)* (Dec. 16, 2005).

guideline 2—"Develop common standards for the sharing of information between and among executive departments and agencies and state, local, and tribal governments, law enforcement agencies, and the private sector"—the 2008 annual report identifies the status of efforts to generate, disseminate, and receive terrorism-related alerts, warnings, and notifications between the federal government and state, local, and tribal stakeholders. Also, the Program Manager laid out annual performance goals that list specific and measurable activities to be accomplished in 2009, such as completing initial efforts to implement the new suspicious activity reporting process—an initiative for streamlining the process for sharing information on suspicious activities or incident information with a potential terrorism nexus between federal, state, local, and tribal partners. Nevertheless, while the performance goals incorporate some quantitative data for assessing progress, they continue to focus on counting activities rather than measuring outcomes. For example, one performance goal states that agencies will increase fusion centers' access to terrorism-related information and ISE capabilities but does not define what this goal means and provide information on how it will be measured. Such information might include identifying the level of access centers currently have to information for use as a baseline from which to measure progress, the target increase agencies are expected to achieve, and how much achieving this goal is expected to improve sharing. While the activities identified in the performance goals and the information provided through the performance measures will likely enhance the fabric of what will ultimately be the ISE, they do not yet identify the overall road map for the ISE and provide answers to key questions regarding what the ISE will include and will not include and how the ISE will function in, for example, the next 3 years.

We appreciate that the ISE and information sharing for protecting the homeland against terrorism is a complex and ever-evolving challenge, making development of a road map for the ISE with which to assess progress, hold stakeholders accountable, and provide Congress and the public with assurance that efforts are being taken to strengthen information sharing ever more important. Therefore, to help ensure that the ISE is on a measurable track to success, we recommended that the Program Manager, with full participation of relevant stakeholders (e.g., agencies and departments on the ISE), (1) more fully define the scope and specific results to be achieved by the ISE along with the key milestones and individual projects or initiatives needed to achieve these results; and (2) develop a set of performance measures that show the extent to which the ISE has been implemented and sharing improved—including, at a minimum, what has been and remains to be accomplished—so as to more

effectively account for and communicate progress and results. The Program Manager generally agreed with these recommendations. In an effort to address these concerns, the Program Manager recently noted in the 2008 annual report that as the ISE matures, he expects the performance management approach will itself mature to move from measuring individual agency progress to measuring the overall performance of the ISE.

Fusion Centers Vary in Their Characteristics, and Federal Efforts Are Under Way That Address Many of the Challenges That Centers Reported Encountering

After September 2001, state and local governments began to establish fusion centers to improve information sharing across levels of government and varying disciplines and to prevent terrorism or other threats. By September 2007, almost all states and several local governments had established, or were in the process of establishing, fusion centers. As we reported in October 2007, these centers varied in their level of maturity, capability, and characteristics. For example, while some centers were just starting out, officials in many (43 of the 58) fusion centers we contacted described their centers as operational. Of these operational centers, 9 opened in the couple of years after September 2001, while 34 opened since January 2004. In terms of capability, we reported that these centers ranged from a center with analysts and access to networks and systems from DHS, FBI, and state and local entities operating at a Top Secret level to a center that had just appointed an officer in charge and lacked access to any of these federal networks and systems. However, our work showed that most of the operational fusion centers we contacted had adopted scopes of operations and missions that included more than just counterterrorism-related activities. For instance, officials in just over half of the operational centers we contacted said that their scopes of operations included all-crimes or all-crimes and terrorism, and several noted the link between crimes and terrorism as a rationale for adopting a broader scope of operations. Officials in about half of the operational centers said that their centers included all-hazards information, such as that related to public health and safety or emergency response. Overall, center officials we contacted during our review told us that adopting a broader focus than counterterrorism helped provide information about all threats, and including additional stakeholders that could provide staff and support could help increase the centers' sustainability. In terms of organization and partnerships, law enforcement entities, such as state police, were the lead or managing agencies in the majority of the centers we contacted. While the centers varied in their staff sizes and partnerships with other agencies, the majority of the operational fusion centers we contacted had federal personnel, including staff from DHS's Office of

Intelligence and Analysis or the FBI, assigned to them as of September 2007.

In our October 2007 report, we identified a variety of challenges—many of which were related to information sharing—that fusion center officials reported encountering in establishing and operating their centers. Among these challenges were managing the high volume of information and the multiple systems and networks, obtaining specific and clear guidance and training on operational issues, obtaining and retaining qualified personnel, and securing federal grant or state and local funding for center operations over the long term. We also reported that to help address these challenges, the Program Manager for the ISE, DHS, and the Department of Justice (DOJ) had several efforts under way, and as we reported in April 2008,[11] many of these efforts were ongoing.

- The Program Manager for the ISE along with DHS and DOJ have efforts under way to streamline systems, including reviewing the most commonly used sensitive but unclassified systems to examine users' needs to identify potential areas in which to streamline system access.[12] In addition, these agencies are taking steps to improve the quality and flow of information through the establishment of the Interagency Threat Assessment and Coordination Group, which became a statutorily mandated body by the 9/11 Commission Act.[13] The group is to include state, local, and tribal representative detailees who are to provide a nonfederal perspective to the intelligence community to produce clear, relevant, federally coordinated terrorism-related information products intended for dissemination to state, local, and tribal officials and to the private sector. In April 2008, we reported that four state and local law enforcement representatives had been detailed to this group. Further, the group's advisory council has been focusing on recruitment for next year's detailees and determining a concept of operations for a detailee fellowship program, according to the ISE 2008 annual report.

[11]GAO-08-636T.

[12]These systems include DHS's Homeland Security Information Network, DOJ's Law Enforcement Online, and the Regional Information Sharing Systems, which is a nationwide initiative to share sensitive but unclassified criminal intelligence among law enforcement, first responders, and private sector stakeholders.

[13]See Pub. L. No. 110-53, § 521, 121 Stat. at 328-32 (adding section 210D to subtitle A, title II of the Homeland Security Act, Pub. L. No. 107-296, 116 Stat. 2135).

- The Program Manager, DHS, and DOJ have taken steps to develop specific, clear guidance and provide technical assistance and training. For example, they have outlined federal and fusion center roles and responsibilities in the *National Strategy for Information Sharing: Success and Challenges in Improving Terrorism-Related Information*, which the administration issued in October 2007. They have also disseminated specific guidance in the form of baseline capabilities that outline minimum operational standards for centers to ensure that they have the necessary structures, procedures, and tools in place to support gathering, processing, analysis, and dissemination of terrorism-related information. In addition, DHS and DOJ's technical assistance program for fusion centers offers training and guidance on, among other things, operational issues such as establishing a privacy and civil liberties policy. These agencies along with the Program Manager for the ISE and others have also sponsored regional and national conferences designed to support fusion centers and provide information about ongoing federal efforts.

- To facilitate information sharing and support fusion centers, DHS and the FBI have deployed personnel, including intelligence officers and special agents. We reported in April 2008 that according to these agencies, DHS had deployed 23 officers to fusion centers and had plans to place officers in as many as 35 centers by the end of fiscal year 2008, and the FBI had assigned about 200 personnel to 44 fusion centers.[14]

- In terms of funding, DHS reported that from fiscal years 2004 through 2007, about $257 million in DHS grant funds supported information sharing and intelligence activities,[15] including 415 projects designated by states and territories for intelligence and fusion center initiatives.

Despite DHS and FBI efforts to deploy personnel to fusion centers and DHS's grant funding, fusion center officials were concerned about long-term sustainability—both the extent of federal support they could expect as well as the roles of their state or local jurisdictions. For example, we reported in October 2007 that challenges for fusion centers included

[14]These deployments may be to fusion centers other than the 58 centers that were included in our October 2007 report.

[15]This includes State Homeland Security Program, Urban Areas Security Initiative, Urban Area Security Initiative Transit Security Program, Law Enforcement Terrorism Prevention Program, Citizen Corps Program, Emergency Management Performance Grants, Metropolitan Medical Response System, Buffer Zone Protection Program, Trucking Security Grant Program, and Transit Security Program grant funding.

uncertain or declining federal funding, finding adequate funding for specific components of their centers' operations, and obtaining state or local funding. One of the specific funding challenges fusion center officials cited was time limits on the use of grant funds for personnel. Some officials expressed concerns about maintaining their personnel levels, such as the 2-year limit on the use of fiscal year 2007 DHS grant funds for personnel. This limit made retaining personnel challenging because state and local agencies may lack the resources to continue funding the position, which could affect the centers' ability to continue to operate. In our October 2007 report, we recommended that the federal government determine and articulate its long-term fusion center role and whether it expects to provide resources to help ensure their sustainability. The *National Strategy for Information Sharing* stated that the federal government will support the establishment of fusion centers and help sustain them through grant funding, technical assistance, and training to achieve a baseline level of capability. Similarly, the 9/11 Commission Act includes provisions for allowing grant funding through the State Homeland Security and Urban Areas Security Initiative grant programs to be used for a variety of fusion-related activities, including paying salaries for personnel. However, we reported in April 2008 that there was still uncertainty among fusion center officials about how specifically the federal government was planning to assist state and local governments in sustaining their fusion centers, in particular with respect to grant funding for intelligence analysts. Specifically, under the fiscal year 2008 Homeland Security Grant Program guidance, costs associated with hiring intelligence analysts were allowable for 2 years but were limited to the hiring of new analysts. After 2 years, states and urban areas are responsible for supporting the sustainment costs of those intelligence analysts. Legislation introduced in May 2008, and reported by the House Committee on Homeland Security July 10, 2008, seeks to clarify what constitutes allowable costs under these grants.[16] The committee found that the federal government has placed restrictions on the use of these funds that make long-term planning for fusion centers unmanageable. The proposed legislation would, among other things, permit states and localities receiving funds under either the State Homeland Security Program or the Urban Areas Security Initiative program to use grant funds toward salaries

[16]Personal Reimbursement for Intelligence Cooperation and Enhancement of Homeland Security Act, H.R. 6098, 110th Cong. (2008) (proposing amendments to the Homeland Security Act of 2002, Pub. L. No. 107-296, 116 Stat. 2135, to improve the financial assistance provided to state, local, and tribal governments for information sharing activities). See also H.R. Rep. No. 110-752 (July 10, 2008).

for analysts regardless of whether the analysts are current or new full-time employees or contract employees and without limitations on the period of time that these analysts can serve under the awarded grants. In addition, to support the establishment and sustainment of a national integrated network of fusion centers, among the federal government's planned activities, the ISE 2008 annual report includes the development of a national investment strategy to sustain fusion center operations, including a delineation of current and recommended future federal and nonfederal costs.

A New Policy Is Intended to Streamline Processes for Sharing Sensitive but Unclassified Information

In March 2006, we reported on a survey of 26 federal agencies[17] that showed they were using more than 50 different designations to protect information that they deem critical to their missions—such as law enforcement sensitive, for official use only, and unclassified controlled nuclear information. At that time, there were no governmentwide policies or procedures that described the basis on which agencies should designate, mark, and handle this information. In this absence, each agency determined what designations to apply. We reported that such inconsistency can lead to challenges in information sharing. In fact, more than half of the agencies reported encountering challenges in sharing sensitive but unclassified information. For example, 11 of the 26 agencies reported concerns about the ability of other parties to protect sensitive but unclassified information, while another 6 of these agencies said that the lack of standardized criteria for defining what constitutes sensitive but unclassified information was a challenge in their sharing efforts. In addition, we found that the prevalence of designations can confuse those receiving the information, such as local and state law enforcement agencies, which in turn must understand and safeguard the information according to each federal agency's rules. This is problematic because, as we found, most agencies did not determine who and how many employees could make sensitive but unclassified designations, provide them training on how to do so, or perform periodic reviews of how well their practices are working. Moreover there were no governmentwide policies that

[17]As identified in our March 2006 report (see GAO-06-385), these federal agencies were generally selected because they are defined as those subject to the Chief Financial Officers Act. In addition, we also included the Federal Energy Regulatory Commission and the U.S. Postal Service because our previous experience with these agencies indicated that they used sensitive but unclassified designations.

required such internal control practices.[18] We reported that if guidance and monitoring is not provided, there is a probability that the designation will be misapplied, potentially restricting material unnecessarily or resulting in dissemination of information that should be restricted. Therefore, we recommended the issuance of a policy that consolidates sensitive but unclassified designations where possible and addresses their consistent application across agencies, as well as a directive requiring that agencies have in place internal controls that meet our *Standards for Internal Control in the Federal Government*—including implementing guidance, training, and review processes.[19]

Consistent with our recommendations and the President's December 2005 mandates calling for standardization of sensitive but unclassified information designations, on May 9, 2008, the President issued a memorandum that adopted CUI as the single categorical designation used for sensitive but unclassified information throughout the executive branch.[20] Specifically, CUI refers to information that is outside the standard National Security Classification system (e.g., Secret, Top Secret, etc.) but that is (1) pertinent to the national interests of the United States or to the important interests of entities outside the federal government and (2) under law or policy requires protection from unauthorized disclosure, special handling safeguards, or set limits on exchange or dissemination. Furthermore, the memo outlined a framework for designating, marking, safeguarding, and disseminating information identified as CUI. In doing so, the memo outlines the following three markings:

- Controlled with standard dissemination, meaning the information requires standard safeguarding measures that reduce the risks of unauthorized or inadvertent disclosure. Dissemination is permitted to the extent that it is reasonably believed that it would further the execution of a lawful or official purpose.

[18]Internal controls are an integral component of an organization's management that provides reasonable assurance that the following objectives are achieved: (1) effectiveness and efficiency of operations, (2) reliability of financial reporting, and (3) compliance with applicable laws and regulations. See GAO, *Standards for Internal Controls in Federal Government*, GAO/AIMD-00-21.3.1 (Washington, D.C.: Nov. 1999).

[19]GAO-06-385.

[20]See Presidential Memorandum, *Memorandum for the Heads of Executive Departments and Agencies: Designation and Sharing Controlled Unclassified Information* (May 9, 2008).

- Controlled with specific dissemination, meaning the information requires safeguarding measures that reduce the risks of unauthorized or inadvertent disclosure. Material contains additional instructions on what dissemination is permitted.

- Controlled enhanced with specified dissemination, meaning the information requires safeguarding measures more stringent than those normally required since the inadvertent or unauthorized disclosure would create the risk of substantial harm. Material contains additional instructions on what dissemination is permitted.

The memo made NARA responsible for overseeing and managing the implementation of the CUI framework. In response, NARA established the CUI Office to accomplish the new tasks associated with implementing the CUI policy. The new office is to undertake nine steps for the implementation and standardization governing CUI policy. Chief among these are (1) establishing new safeguards and dissemination controls, (2) publishing standards in a new official CUI Registry, (3) monitoring department and agency compliance with CUI policy and standards, (4) establishing required training and an associated training program for departments and agencies, and (5) providing appropriate documentation regarding the CUI framework to Congress; state, local, tribal, and private entities; and foreign partners. Issuing the new policy and laying out responsibilities is a good first step. Our work has demonstrated that monitoring agencies' compliance with CUI policies and standards to ensure that they implement guidelines, training, and internal controls will help ensure that the policy is employed consistently across the federal government and facilitate the sharing of terrorism-related information.

Our November 2007 review of TSA's program on managing sensitive security information[21] showed that in response to our prior recommendations on establishing guidance and procedures for using TSA regulations to determine what constitutes sensitive security information, TSA's program had instituted key components critical for the sharing of unclassified sensitive information and could serve as a model to guide other agencies' implementation of CUI. TSA has also shared its criteria and

[21]Sensitive security information is a statutorily established category of sensitive but unclassified information that includes information obtained or developed in the conduct of security activities that, for example, would be detrimental to transportation security. See 49 U.S.C. § 114(s); see also 49 C.F.R. pt. 1520. Sensitive security information is not subject to the CUI requirements.

examples used to help employees determine what is sensitive security information with other DHS components. Representatives we interviewed from these other DHS components have recognized opportunities to adapt TSA's criteria to their offices' unique needs. Furthermore, TSA has appointed sensitive security information coordinators at all program offices, such as the Office of Law Enforcement/Federal Air Marshal Service, among other things, to implement sensitive security information determination policies. TSA's Office for Sensitive Security Information is in the process of providing training to all TSA employees and contractors on how to handle sensitive security information in accordance with its newly adopted policies and procedures. The office has a "train the trainer" program that instructs sensitive security information program managers and coordinators who are then expected to train appropriate staff in their respective agencies and programs. Several aspects of the sensitive security information training program that we evaluated are consistent with GAO-identified components of a strategic training program.[22] Within this effort, TSA also has processes for responding to requests for sensitive security information from federal, state, local, and tribal government entities. Furthermore, TSA's sensitive security information program has internal controls in place that are consistent with governmentwide requirements and respond to our recommendation. For example, TSA is in the process of conducting an audit to identify existing sensitive security information and its use, as well as evaluating a portion of records marked as containing such information.

Mr. Chairman, this concludes my statement. I would be pleased to answer any questions that you or other members of the committee may have at this time.

Contacts and Acknowledgments

For further information on this testimony, please contact Eileen Larence at (202) 512-8777 or larencee@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this statement. Individuals making key contributions to this testimony include Susan Quinlan, Assistant Director; Mary Catherine Hult, Assistant Director; Joseph Cruz; and Anish R. Bhatt.

[22]GAO, *A Guide for Assessing Strategic Training and Development Efforts in the Federal Government*, GAO-04-546G (Washington, D.C.: Mar. 2004).

Testimony
Before the Senate Committee on Homeland Security and Governmental Affairs

Information Sharing: Connecting the Dots at the Federal, State, and Local Levels

Statement of Ambassador Thomas E. McNamara
Program Manager
Information Sharing Environment

I. ***Introduction***

Chairman Lieberman, Ranking Member Collins, and Members of the Committee, let me begin by taking this opportunity to thank you for your continued support of our efforts to build an information sharing environment.

In June 2008, the second Annual Report to the Congress on the Information Sharing Environment (ISE) was submitted in accordance with requirements in Section 1016(h) of the *Intelligence Reform and Terrorism Prevention Act of 2004.* The Report, attached here, describes the state of the ISE and highlights areas where there has been measurable progress in improving information sharing and demonstrates the value of the ISE to the Nation's broader counterterrorism (CT) mission. In particular, the President's October 2007 *National Strategy for Information Sharing* (NSIS) reinforced the importance of information sharing as a national priority. The NSIS serves as an integrating document for all prior terrorism-related information sharing policies, directives, plans, and recommendations and provides a national framework against which to implement the ISE.

The Report reflects the collective accomplishments and challenges of an information sharing partnership of Federal and non-Federal stakeholders vested in the improvement of terrorism-related information sharing. It also highlights agency initiatives that stand out as best practices in information sharing and help form the fabric of the ISE.

II. ***Progress in Improving Information Sharing***

The enactment of IRTPA in December 2004 signaled the start of a major effort to ensure that barriers to information sharing were removed and that best practices were leveraged and used across Federal agencies. The breadth and complexity of the information sharing challenge should not be underestimated. Information silos, cultural issues, and other barriers that inhibit sharing still exist today. However, as demonstrated through the alignment of NSIS "Core Principles and Understandings" to ISE accomplishments, significant progress has already been made. Examples reveal how broadly information sharing in general, and the ISE in particular, have begun to permeate our institutions of government.

II.1. ***Providing a Coordinated Federal Voice to State, Local, and Tribal Governments***

An absence of consistent messaging from Federal agencies to their State, Local, Tribal (SLT) and private sector partners historically hindered the establishment of a productive, national information sharing partnership. Today, however, implementation of the Presidential Guideline 2 recommendations, incorporation of those recommended activities into the NSIS, and the codification of a number of those activities into law by Congress, are changing this paradigm. SLT and private sector stakeholders now benefit from a process that includes the Interagency Threat Assessment and Coordination Group at the National Counter Terrorism Center, which is dedicated to ensuring that there is a unified voice among Federal agencies tailored to their special needs. In addition, a formal process now exists for the exchange of coordinated terrorism information products between the Federal Government and its non-Federal partners.

II.2. ***Creating a Common Framework for the Marking and Handling of Controlled Unclassified Information***

More than 100 unique SBU markings exist across the government, impeding the access and availability of this information to its appropriate recipients. With the President's May 2008 memo on the CUI framework, the White House mandated a single marking and handling framework within the ISE for implementation by all Federal Government agencies. Adoption of this framework allows Federal and non-Federal stakeholders to more efficiently share CUI in a manner consistent with applicable privacy and civil liberties laws.

II.3. ***Promulgating a Comprehensive Set of Privacy Guidelines***

IRTPA and the NSIS both mandate that information sharing be consistent with the need to protect civil liberties and information privacy. Prior to these authorities, the Federal Government lacked consistent guidelines for the protection of privacy and other legal rights in the sharing of information. To address this need, the President mandated the development and implementation of a set of Privacy Guidelines for the ISE. Released in the fall of 2006, these guidelines maintain and build upon existing privacy protections while continuing to enhance the sharing of terrorism-related information between agencies at all levels of government.[1]

II.4. ***Adopting a Collaborative Approach to Information Sharing***

The release this past year of the Intelligence, Defense, and Homeland Security information sharing strategies signaled strong, continuing information sharing collaboration within communities. However, IRTPA, Executive Orders, and the NSIS also require an integrated, cross-community approach to information sharing; intra-agency or single community solutions alone no longer suffice. Since last year's report, significant progress has been made in removing information sharing obstacles within the Federal Government and implementing solutions that ensure Federal, SLT and private sector participants receive the information they need to fulfill their CT missions. These efforts, including the national process for gathering, processing, and sharing terrorism-related ISE Suspicious Activity Reports (SAR), are increasingly more visible and cut across agencies and communities of interest to involve all levels of government and the private sector.

II.5. ***Implementing a Common Architectural Framework for the ISE***

To integrate, sustain, and institutionalize improvements, it is necessary to establish an enduring framework that becomes ingrained in the everyday functions of government. Released last fall, the ISE Enterprise Architecture Framework (ISE EAF) is driven by business process improvements and is a vehicle to make these improvements permanent. In direct response to IRTPA direction, the ISE EAF provides a common architectural structure for agencies to incorporate their information sharing capabilities into the ISE. In addition, because it breaks new ground in several areas, other

---

[1] *ISE Privacy Guidelines*, the Office of the Program Manager for the Information Sharing Environment (December 4, 2006). Available online at: http://www.ise.gov/docs/privacy/PrivacyGuidelines20061204.pdf.

information sharing stakeholders —notably the national health care community—are now leveraging the ISE EAF to help develop their own enterprise architectures.

II.6. ***Issuing Common Terrorism Information Sharing Standards (CTISS)***

Prior to the enactment of IRTPA, a few terrorism-related information sharing standards and sharing practices existed within certain agencies, but they were not always applied consistently, nor did they reach outside the agency. Today, the CTISS Program is designed for interagency, business process-driven, performance-based "common standards" for preparing terrorism information for maximum distribution and access. It also enables the acquisition, access, retention, production, use, management, and sharing of terrorism-related information within the ISE. The first standard issued under the CTISS Program, the ISE SAR Functional Standard, has already shown the value of a common format -- incorporating explicit privacy safeguards -- to the sharing of suspicious activity reports among Federal and SLT partners.

In late 2007, the PM-ISE, National Information Exchange Model (NIEM), Department of Defense (DoD) Universal Core (UCORE), and Office of the Director of National Intelligence (DNI) Chief Information Officer program offices formed a multi-agency partnership for developing new, converged information exchange standards supporting the Law Enforcement (LE), Homeland Security, Defense, and Intelligence communities. Plans for 2008 include incorporating this new multi-community NIEM-UCORE information exchange standard into CTISS as a foundation for developing and implementing new and better ISE standards.

II.7. ***Developing Standardized ISE-wide Participant Training***

Organizational and community cultures across the ISE vary widely, and information sharing is not yet viewed as a required behavior. To further promote such behavior, and create a common understanding and shared awareness of the ISE, the PM-ISE has issued an "ISE 101" training module. Some ISE organizations have already instituted extensive training about information sharing and will adapt this course to their existing training programs. Other ISE organizations will use this as the foundation for developing organization-specific information sharing training. This training, coupled with continued efforts to include information sharing as a formal evaluation factor in personnel performance reports and agency incentive programs, is designed to help move the traditional "need to know" culture to one based on a "responsibility to provide."[2]

III. ***The Way Ahead***

The NSIS documents the progress made in information sharing and describes the Administration's "expectations and plans for achieving improvements in the gathering and sharing of information related to terrorism."[3] It reaffirms the vision, goals, and strategies embodied in the ISE Implementation Plan (IP) while acknowledging that today's sharing environment serves as a platform from which to continually improve the

---

[2] *United States Intelligence Community Information Sharing Strategy*, the Office of the Director of National Intelligence (February 2008), p. 2.
[3] *National Strategy for Information Sharing (NSIS)*, White House (October 2007), p. 2.

sharing of terrorism-related information among all levels of government, the private sector, and foreign partners.[4]

In the attached report I have provided Congress the 2009 Performance Goals. ISE performance management efforts linking these goals to supporting objectives and measures will bring the ISE even closer to complying with the Presidential guidelines and the NSIS. This linkage will also provide the PM-ISE and the Information Sharing Council (ISC) a means to better determine whether ISE initiatives are having their intended effect. ISC member agencies will use this assessment to identify areas where they can better build their capacity for information sharing. A line of sight from the 2009 Performance Goals to further maturation of specific ISE activities identified in the President's Guidelines and Requirements will provide the PM-ISE and the ISC with data to demonstrate the ISE's value to the next Administration, Congress, and beyond.

ATTACHMENT 1: *Second Annual Report to the Congress on the Information Sharing Environment June 2008*

---

[4] *ISE Implementation Plan (ISE IP)*, Office of the Program Manager for the Information Sharing Environment (November 2006). The *ISE Implementation Plan* contained nearly 100 short- and long-term actions to improve the sharing of terrorism information. These actions are organized into several high-level themes including ISE operational capabilities, architecture and standards; sharing with Federal and non-Federal partners; incentives/disincentives; training; protecting privacy and civil liberties; terrorism information handling; ISE performance management; and ISE planning, programming, and budgeting.

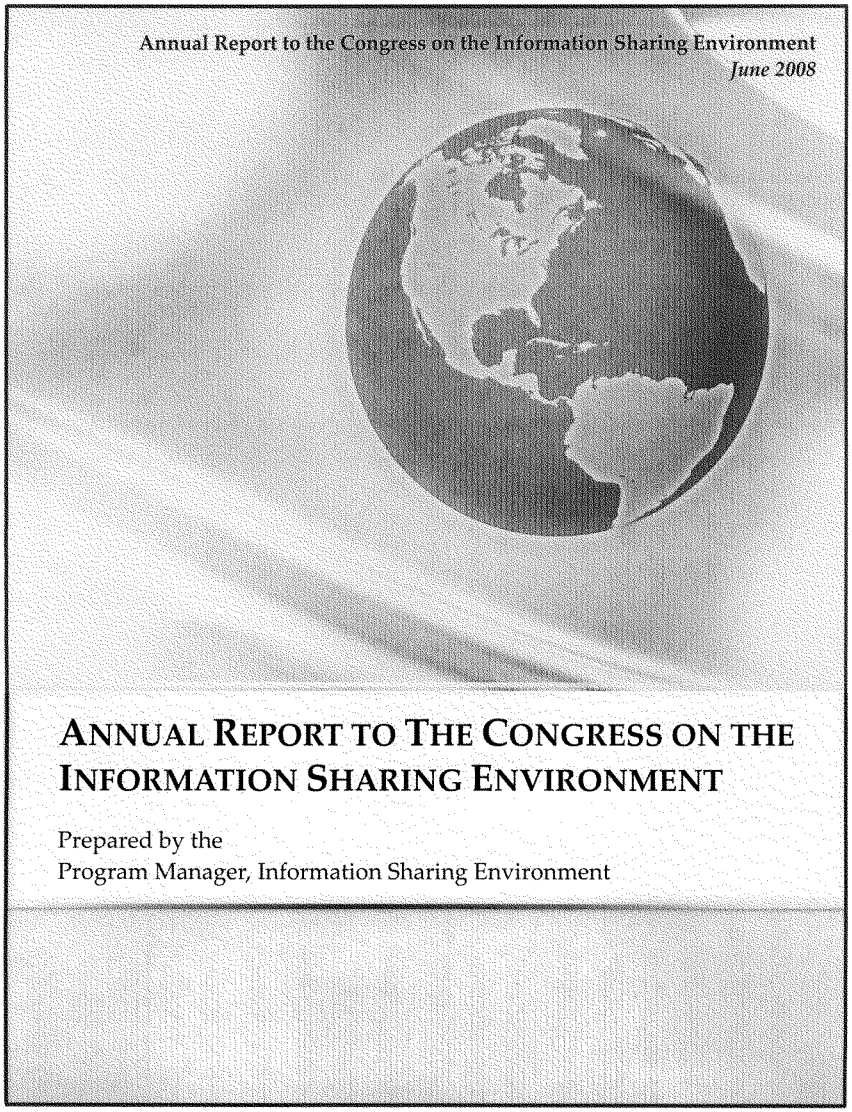

Annual Report to the Congress on the Information Sharing Environment
June 2008
ANNUAL REPORT TO THE CONGRESS ON THE INFORMATION SHARING ENVIRONMENT
Prepared by the
Program Manager, Information Sharing Environment

TABLE OF CONTENTS

List of Figures iii

List of Tables iii

Foreword v

Executive Summary vii
Implementation of Presidential Information Sharing Guidelines vii
Leveraging Ongoing Information Sharing Efforts ix
Promoting a Culture of Information Sharing x
Way Ahead x

1 Introduction 1
1.1 Purpose and Scope 1
1.2 Overview of the ISE 1
1.2.1 Background 1
1.2.2 The ISE: A Partnership of Five Communities 2
1.2.3 Achieving ISE Operational Capabilities 3
1.3 The Reality of an Information Sharing Environment 4
1.4 ISE Performance Management 6
1.4.1 Introduction 6
1.4.2 Performance Assessment Results 8

2 Establishing Information Sharing Standards 13
2.1 2007-08 Highlights 13
2.2 ISE Enterprise Architecture Framework 13
2.3 Common Terrorism Information Sharing Standards 15
2.4 ISE Shared Spaces 16
2.5 Building a Trusted Environment 17
2.5.1 ISE Risk Management Framework 17
2.5.2 Improved Security Practices 18
2.6 Broader Application of ISE EAF and CTISS 19
2.7 Next Steps 20
2.7.1 Architecture and Standards 20
2.7.2 Building a Trusted ISE 21

3 Sharing Within, Across, and Between Levels of Government 23
3.1 2007-08 Highlights 23
3.2 Sharing Information with State, Local, and Tribal Governments 24
3.2.1 The Interagency Threat Assessment and Coordination Group 24
3.2.2 State and Major Urban Area Fusion Centers 25
3.2.3 Tribal Governments 26

3.3 Sharing Information with the Private Sector 26
3.4 Improving ISE Business Processes 27
3.4.1 Suspicious Activity Reporting 28
3.4.2 Terrorist Watch Lists 30
3.4.3 Terrorism-Related Alerts, Warnings, and Notifications 31
3.5 Terrorist-Related WMD Information in the ISE 32
3.6 Next Steps 32
3.6.1 Sharing Information with SLT Governments and the Private Sector 32
3.6.2 Suspicious Activity Reporting 33
3.6.3 Terrorist Watchlists 33
3.6.4 Alerts, Warnings, and Notifications 33
3.6.5 Terrorist-Related WMD Information 34

4 Standardizing Procedures for Sensitive But Unclassified Information 35
4.1 2007-08 Progress 35
4.1.1 Standardizing Procedures for Sensitive But Unclassified Information 35
4.1.2 Protected SBU Transport 36
4.2 Next Steps 37
4.2.1 Implementing the CUI Framework 37
4.2.2 Protected Transport 37

5 Sharing with Foreign Partners 39
5.1 2007-08 Progress 39
5.2 Next Steps 40

6 Protecting Privacy & Other Legal Rights 41
6.1 2007-08 Progress 41
6.2 Next Steps 42

7 Leveraging Ongoing Information Sharing Efforts 43
7.1 ISE Governance 44
7.2 ISE Investment Planning 45
7.2.1 The ISE Planning Cycle 45
7.2.2 Assessing Costs for ISE Priorities 46

8 Promoting a Culture of Information Sharing 47
8.1 2007-08 Progress 47
8.2 Next Steps 48

9 2009 ISE Performance Goals 51

Appendix A – Summary of the Alignment Between the NSIS and ISE Accomplishments 53

Appendix B – Acronyms and Abbreviations 55

LIST OF FIGURES

Figure 1-1. View of the ISE as a Partnership of Five Communities 3
Figure 1-2. Example Law Enforcement Information Flow 6
Figure 1-3. ISE Performance Management Evolves as the ISE Matures 7
Figure 2-1. Overview of the ISE Enterprise Architecture Framework 14
Figure 2-2. The ISE Risk Management Framework 18
Figure 7-1. ISE Annual Planning Cycle 45

LIST OF TABLES

Table 1-1. 2008 ISE Performance Goals 8
Table 9-1. 2009 ISE Performance Goals 51

Foreword

Message From the Program Manager, Information Sharing Environment

On behalf of the President and the Director of National Intelligence, I am pleased to present this second *Annual Report to the Congress on the Information Sharing Environment (ISE)*. We believe it demonstrates a solid record of accomplishment by the Office of the Program Manager, the many agencies represented on the Information Sharing Council, and our partners in State, local, and tribal (SLT) governments. In the past year we have made significant progress in a number of important areas of information sharing. Issuance of a new framework for marking and handling Controlled Unclassified Information, establishment of the Interagency Threat Assessment and Coordination Group at the National Counterterrorism Center, completion of a functional standard for terrorism-related suspicious activity reporting, and publication of the first version of an enterprise architecture framework for the ISE are only a few of the important achievements.

Notwithstanding these achievements, there is still much more to be done. In particular, Information Sharing Council (ISC) member agencies must work to fully implement the ISE; assure full participation by our SLT partners; and help secure and make safe our communities and nation by effectively sharing information. So, in addition to describing 2007-08 accomplishments, the Report outlines the status, outcomes and activities that are needed to continue to improve information sharing.

Thomas E. McNamara
Program Manager, Information Sharing Environment

Executive Summary

This second *Annual Report to the Congress on the Information Sharing Environment (ISE)* is submitted in accordance with requirements in Section 1016(h) of *the Intelligence Reform and Terrorism Prevention Act of 2004*, as amended (IRTPA).[1] This Report describes the state of the ISE, highlights areas where there has been measurable progress in improving information sharing, and demonstrates the value of the ISE to the Nation's broader counterterrorism (CT) mission. In particular, the President's October 2007 *National Strategy for Information Sharing* (NSIS) reinforced the importance of information sharing as a national priority. The NSIS integrates all prior terrorism-related information sharing policies, directives, plans, and recommendations and provides a national framework against which to implement the ISE.

The enactment of IRTPA in December 2004 signaled the start of a major effort to ensure that barriers to information sharing were removed and that best practices were employed across Federal agencies. While the complexity of the information-sharing challenge should not be underestimated, significant progress has been made. This Report addresses progress in information sharing to date while revealing how the paradigm of information sharing – and the ISE in particular – has broadly permeated our institutions of government.

ISE accomplishments are significant when viewed according to the original mandate, set forth in the President's December 16, 2005 *Memorandum to the Heads of Executive Departments and Agencies on the Guidelines and Requirements in Support of the Information Sharing Environment,* which set forth the Presidential Information Sharing Guidelines. These guidelines are implemented by leveraging ongoing information sharing efforts and supported by promoting a culture of information sharing.

Implementation of Presidential Information Sharing Guidelines

As of this Report, recommendations for the five Presidential guidelines are complete and approved by the President for implementation, and actual implementation is well underway across all five areas. The following is a summary of that status; additional details are provided in the body of this Report.

[1] *Intelligence Reform and Terrorism Prevention Act of 2004* (IRTPA), as amended, P.L. 108-458 (December 17, 2004) §1016(b)(1)(A). The scope of the ISE was originally limited to "terrorism information" as defined in Section 1016. In August 2007, The *Implementing Recommendations of the 9/11 Commission Act of 2007* (P.L. 110-53), included amendments to Section 1016 that expanded the scope of the ISE to explicitly include homeland security and weapons of mass destruction information and identified additional ISE attributes. It also endorsed and formalized many of the recommendations developed in response to the Presidential information sharing guidelines, such as the creation of the Interagency Threat Assessment and Coordination Group, and the development of a national network of State and major urban area fusion centers.

1. *Defining Common Standards for How Information is Acquired, Accessed, Shared, and Used within the ISE.* In October 2007, the Office of the Program Manager for the Information Sharing Environment (PM-ISE) and the interagency Information Sharing Council (ISC) formally established the Common Terrorism Information Sharing Standards (CTISS) Program. The first common ISE standard (the *ISE Suspicious Activity Reporting (SAR) Functional Standard*) was issued in January 2008 and others are under development. In direct response to IRTPA direction, the PM-ISE released the *ISE Enterprise Architecture Framework* (ISE EAF) last fall. The ISE EAF provides a common architectural structure for agencies to use as they implement these information sharing standards.

2. *Developing a Common Framework for the Sharing of Information Between and Among Executive Agencies and State, Local, and Tribal (SLT) Governments, Law Enforcement Agencies, and the Private Sector.* Established at the National Counterterrorism Center (NCTC), an Interagency Threat Assessment and Coordination Group (ITACG) facilitates the production of "federally coordinated" terrorism-related information products intended for dissemination to SLT officials and private sector partners. Considerable progress has also been achieved at developing a national network of state and major urban area fusion centers.

3. *Standardizing Procedures for Sensitive But Unclassified (SBU) Information.* Developed by an interagency Coordinating Committee and implemented through the President's May 9, 2008 *Memorandum for the Heads of Executive Departments and Agencies on the Designation and Sharing of Controlled Unclassified Information (CUI),* a common framework will streamline the designation, marking, safeguarding, and dissemination of CUI within the ISE.[2]

4. *Facilitating Information Sharing Between Executive Agencies and Foreign Partners.* In March 2008, the PM-ISE and ISC established an interagency committee to guide implementation of these recommendations. The committee provides tools and other mechanisms to assist Federal agencies in developing and managing foreign sharing agreements.

5. *Protecting the Information Privacy Rights and Other Legal Right of Americans.* ISE Privacy Guidelines and implementing procedures have been issued, and an ISE Privacy Guidelines Committee (PGC) established, to assist agencies in implementation. Released by the PM-ISE in the fall of 2006, the promulgated guidelines maintain and build upon existing privacy protections while continuing

[2] *Memorandum for the Heads of Executive Departments and Agencies: Designation and Sharing of Controlled Unclassified Information (CUI),* White House (May 9, 2008). Available online at: http://www.whitehouse.gov/news/releases/2008/05/20080509-6.html.

to enhance the sharing of terrorism-related information between agencies at all levels of government.[3]

Leveraging Ongoing Information Sharing Efforts

The PM-ISE, in consultation with the ISC, has identified and leveraged ongoing information sharing efforts to align with the Presidential Guidelines and extended these efforts to cover all ISC participant agencies. The PM-ISE has also worked with agencies to build their capacity for information sharing by having agencies take greater ownership of these efforts, and ultimately, of targeted outcomes and out-year performance goals. The PM-ISE has leveraged, enhanced, and extended various existing initiatives, to include:

- Information sharing frameworks and data standards, including the National Information Exchange Model (NIEM) standards and Department of Defense (DoD)-Director of National Intelligence (DNI) Universal Core (UCORE) data standards, as part of the CTISS Program, to facilitate information exchanges (i.e. ISE SAR information) between different domains or communities of interest;
- The Federal Bureau of Investigation (FBI)-sponsored Joint Terrorism Task Forces (JTTFs), combining Federal-State-Local units dedicated to combating terrorism in specific geographical areas;
- State and major urban area fusion centers, many of which are collocated with JTTFs and some of which have Department of Homeland Security (DHS) representation as well; and
- The ISE Governance Structure (described in the ISE Implementation Plan) that provides a framework for coordinating interagency actions and leveraging existing or planned agency initiatives; and
- Federal, SLT, and private sector governance structures such as the Federal Chief Information Officers Council, the Global Justice Information Sharing Initiative (Global), and the National Infrastructure Protection Plan sector partnership model, as mechanisms to provide subject matter expertise and contribute to the development of ISE capabilities.

Sound ISE investment oversight and planning are important parts of managing the ISE and leveraging ongoing information sharing efforts. Coordinated, cross-ISE investment planning provides insight into ISC members' programs and budgets and will help ensure that ISC member agencies include ISE initiatives in their out-year planning and investment efforts. As detailed in Section 7, a standard *ISE Planning Cycle* coordinates the ISE's strategic direction, resource planning, and program oversight. It leverages existing Office of Management and Budget (OMB) processes and procedures to include

[3] *ISE Privacy Guidelines*, the Office of the Program Manager for the Information Sharing Environment (December 4, 2006). Available online at: http://www.ise.gov/docs/privacy/PrivacyGuidelines20061204.pdf.

the steps involved in planning, programming, budgeting, and executing the resources necessary to institutionalize the ISE. Annual ISE investment reviews focus on identifying information sharing costs from larger mission operations costs to ensure that existing resource allocations are properly leveraged as part of the investment planning process.

Promoting a Culture of Information Sharing

Organizational cultures across the ISE vary widely, and information sharing is not viewed across the board as a required behavior. To promote a shared awareness of the ISE and encourage such behavior, the PM-ISE will issue an "ISE 101" training module this summer. The course is intended to give a common understanding of the ISE to all employees who support the CT mission. This training, coupled with continued efforts to include information sharing as a formal evaluation factor in personnel performance reports and agency incentive programs, is designed to help move the traditional "need to know" culture to one based on a "responsibility to provide."[4]

Way Ahead

In addition to chronicling the progress made since September 11th in improving information sharing, the NSIS outlines the steps necessary to ensure that agencies continue to embrace the practice of freely sharing terrorism-related information. In the next year, key milestones include delivery of:

- Functional and technical standards, including a focus on fully-implementing a national standardized process for ISE SAR;
- Technical assistance, training, and policy that furthers the establishment and operational effectiveness of a national integrated network of fusion centers;
- A process that fully aligns ISE budget, planning, and performance activities to OMB and agencies' management and budget processes;
- An implementation plan for the new CUI framework; and
- The continued protection of the privacy and other legal rights of all Americans through further implementation of the ISE Privacy Guidelines.

[4] *United States Intelligence Community Information Sharing Strategy*, the Office of the Director of National Intelligence (February 2008), p. 2.

1 Introduction

1.1 Purpose and Scope

This second *Annual Report to the Congress on the Information Sharing Environment (ISE)* is submitted in accordance with requirements in Section 1016(h) of the *Intelligence Reform and Terrorism Prevention Act of 2004, as amended* (IRTPA).[5] This Report describes the state of the ISE, highlights areas where there has been measurable progress in improving information sharing, and demonstrates the value of the ISE to the Nation's broader counterterrorism (CT) mission. In particular, the President's October 2007 *National Strategy for Information Sharing* (NSIS) reinforced the importance of information sharing as a national priority. The NSIS integrates all prior terrorism-related information sharing policies, directives, plans, and recommendations and provides a national framework against which to implement the ISE.

This Report responds directly to the IRTPA requirement for "a progress report on the extent to which the ISE has been implemented." It reflects the collective accomplishments and challenges of an information sharing partnership of Federal and non-Federal stakeholders vested in the improvement of terrorism-related information sharing. It also highlights individual agency initiatives that stand out as best practices in information sharing and help form the fabric of the ISE.

1.2 Overview of the ISE

1.2.1 Background

Section 1016 of IRTPA defines the ISE as "an approach that facilitates the sharing of terrorism and homeland security information" which "may include any methods determined necessary and appropriate for carrying out this section."[6] The ISE Implementation Plan (IP) sets forth a vision of the environment as "a trusted partnership between all levels of government in the United States, the private sector, and our foreign partners, to detect, prevent, disrupt, preempt, and mitigate the effects of

[5] IRTPA, as amended, op. cit., §1016(b)(1)(A). The scope of the ISE was originally limited to "terrorism information" as defined in Section 1016. In August 2007, The *Implementing Recommendations of the 9/11 Commission Act of 2007* (P.L. 110-53), included amendments to Section 1016 that expanded the scope of the ISE to explicitly include homeland security and weapons of mass destruction information and identified additional ISE attributes. It also endorsed and formalized many of the recommendations developed in response to the Presidential information sharing guidelines, such as the creation of the Interagency Threat Assessment and Coordination Group, and the development of a national network of State and major urban area fusion centers.

[6] Ibid. §1016(a)(2).In the balance of this report, terrorism and homeland security information will be referred to as "terrorism-related information."

terrorism against the territory, people, and interests of the United States of America by the effective and efficient sharing of terrorism information."[7]

These broad descriptions convey the essential point that establishing the ISE is not about building a dedicated information system to support the national CT mission. Rather, it largely entails building on capabilities already in place by adjusting and integrating existing policies, business processes, architectures, standards, and systems to enable the improved sharing of information among all ISE participants. The authors of IRTPA carefully avoided calling the ISE a "system," "information sharing network," or "program," choosing instead the term "environment" to describe the set of conditions that must coalesce through the application of those interrelated policies, business processes, and standards to use existing systems.[8]

1.2.2 The ISE: A Partnership of Five Communities

The ISE IP describes the five primary communities that constitute the ISE: Intelligence, Foreign Affairs, Homeland Security, Law Enforcement, and Defense. To illustrate further, Figure 1-1 depicts these five communities as multi-story buildings within a common neighborhood which contain repositories of terrorism-related information and are connected by walkways and skyways.[9] Each building (representing a single community) also has several distinct but connected floors corresponding to the stakeholders who contribute to that community's counterterrorism efforts—Federal and State, local, and tribal (SLT) governments, private sector entities, and foreign partners. The figure illustrates that stakeholder relationships will vary from one community to another. The Homeland Security community, for example, has a stronger association with SLT and private sector stakeholders than does the Foreign Affairs community which, in turn, must necessarily have much closer ties with foreign partners.

The inner courtyard of Figure 1-1 depicts the essential capabilities that help unify the five communities. Improved policies, business processes, architectures, standards, and systems combine to enable the walkways, skyways, elevators, and staircases of the ISE to provide trusted, efficient, and effective movement of information both inside the buildings and across the neighborhood.

---

7 *ISE Implementation Plan* (November 2006), p. 11.

8 The second Markle Foundation Task Force report, *Creating a Trusted Information Network for Homeland Security* (December 2002) did use the term "network." IRTPA, however, although influenced by the Markle report, eschewed this term in favor of "environment."

9 Both Intelligence Community members and other organizations (sometimes referred to as non-Title 50 agencies) will contribute to these repositories of terrorism-related information.

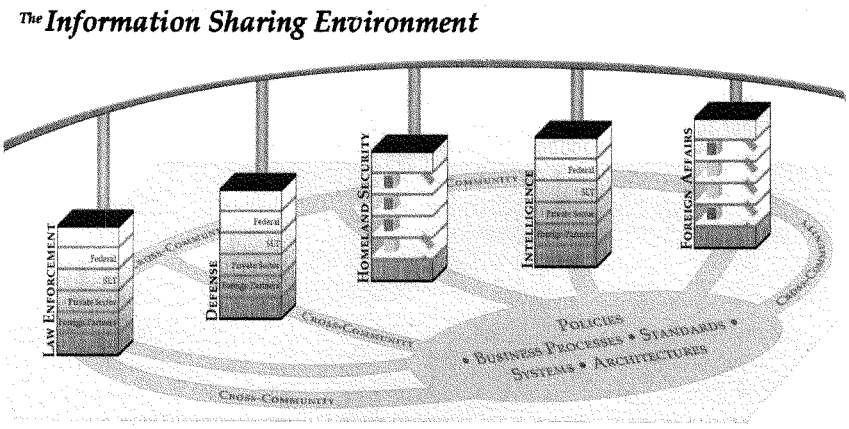


Figure 1-1. View of the ISE as a Partnership of Five Communities

The purpose of the ISE is to *rationalize, standardize, and harmonize* the policies, business processes, architectures, standards, and systems used to share information. Although the ISE strives for much uniformity as possible, actual implementation will vary from one building (community) to another (and even between floors in a building) depending on varied mission needs and immediate capabilities. State and local processes and policies, for example, will not be identical to those of the Federal Government. Nor will the needs of a small town be the same as those of a major urban area. Accordingly, rather than striving to develop identical implementations across the ISE, the intent is to achieve *mostly common* capabilities—based on a common architectural framework supplemented by mostly common laws, regulations, policies, business processes, architectures, standards, and systems—but tailored to ISE participant needs. These capabilities are developed in consultation with the Information Sharing Council (ISC), an interagency advisory body chaired by the Program Manager, Information Sharing Environment (PM-ISE) where participants from each of the five communities help manage and implement the ISE.

1.2.3 Achieving ISE Operational Capabilities

ISE progress is a function of identifying, prioritizing, and measuring continuous improvements to operational capabilities by modifying processes or creating new ones, issuing guidance and standards to ISE participants, providing demonstrable evidence of the effects of these changes through selected information sharing pilots and evaluation environments, and incorporating these improvements into established agency investment and resource management processes.

Achieving the desired outcome and managing the ISE's performance requires a common understanding regarding the problems to be solved, the essential capabilities that constitute the ISE, and the actions needed to ensure that these capabilities are developed and deployed in a manner "consistent with national security and with applicable legal standards relating to privacy and civil liberties."[10] The original blueprint upon which the work of the ISE is based is set forth in the President's December 16, 2005 *Memorandum to the Heads of Executive Departments and Agencies on the Guidelines and Requirements in Support of the Information Sharing Environment,* was further refined in the ISE IP, and fully synthesized in the NSIS. These Presidential guidelines describe ISE capabilities in terms of interrelated policies, business processes, architectures, standards, and systems that, taken together, constitute the sharing environment envisioned in IRTPA and the NSIS—the elements depicted in the courtyard of Figure 1-1.

1.3 The Reality of an Information Sharing Environment

The NSIS requires that the ISE support inclusion of locally generated information because such information is important to the development of statewide and national assessments of terrorist threats.[11] The intent is to make all available information on terrorist-related suspicious activity more widely available to ISE members while protecting information privacy and the legal rights of Americans.

Two important institutions that have spurred progress in enhanced Federal and SLT sharing are:

- The Federal Bureau of Investigation (FBI)-sponsored Joint Terrorism Task Forces (JTTFs), combining Federal-State-Local units dedicated to combating terrorism in specific geographical areas; and
- State and major urban area fusion centers, many of which are collocated with JTTFs, and some of which have Department of Homeland Security (DHS) representation as well.

JTTFs and fusion centers represent a change in culture and a willingness to share information across several levels of government. Both are partnerships that rely on new policies, business processes, architectures, standards, and systems that provide users the ability to access and search information in different databases. Both Federal and SLT law enforcement agencies recognized that they needed to begin to share more detailed information to be effective. This awareness has resulted in the mutual agreement by trusted partners to exchange actual operational data reports, case files, and similar information on both open and closed investigations.

[10] IRTPA, as amended, op cit., §1016(b)(1)(A).
[11] *National Strategy for Information Sharing* (October 2007), pp. A1-6 and A1-7.

This level of sharing required governance boards to develop inter-agency agreements, policies, business processes, and standards—which eventually led to the development of systems requirements. The organizations involved all supported solutions that used distributed sharing methods, allowing each organization to retain its own information and, at the same time, make it available for others to search and retrieve. A distributed approach allows organizations to add, update, or purge data based on all applicable laws and guidance. For example, a State may be able to broadly share information on terrorist-related suspicious activity, but may have to restrict access to certain fields to comply with State privacy laws. Since this information is usually maintained in different formats by each organization, the Law Enforcement Information Sharing Program (LEISP) Exchange Specification (LEXS)—a subset of the National Information Exchange Model (NIEM)— was developed to serve as an "interpreter" between different law enforcement systems, enabling participants on one system to obtain results from others in a familiar format.

At the Federal level, the FBI's Law Enforcement On-line (LEO) system has provided a protected means for sharing Sensitive But Unclassified (SBU) data with regional law enforcement (LE) agency partners through a project originally known as Regional Data Exchange (R-DEx) and subsequently adopted by the Department of Justice (DOJ) for all of its components and renamed OneDOJ. Using LEO, DOJ is integrating the OneDOJ regional partnerships with a new Law Enforcement National Data Exchange (N-DEx) program under the FBI Criminal Justice Information Services (CJIS) Division. In addition, DOJ supports six Regional Information Sharing System (RISS) Network centers that provide tailored support for specialized LE functions to meet regional needs.

The N-DEx development clearly illustrates the value of using common standards. Under N-DEx, exchange of information between law enforcement agencies and CJIS is accomplished by using NIEM standards. In fact, CJIS developed the Information Exchange Package Description (IEPD) before releasing the N-DEx Request for Procurement, allowing the standard to drive subsequent development and implementation activities. Although specific dollar savings are difficult to quantify, vendors are now packaging N-DEx-NIEM compliant applications into off-the-shelf solutions than can easily be adopted by additional jurisdictions, effectively amortizing development costs across a broader customer base.

The Naval Criminal Investigative Service (NCIS) also established the Law Enforcement Information Exchange (LInX) that offers local or regional data hosting capabilities for SLT law enforcement agencies to support their sharing efforts. In the past year, DHS's Immigration and Customs Enforcement (ICE) developed and deployed the ICE Pattern Analysis and Information Collection System (ICEPIC) for integrating homeland security and LE information, and DHS is in the process of establishing relationships to include other departmental LE agencies' information as well.

SLT agencies have taken similar actions in concert with—and in some cases in advance of—Federal initiatives. Numerous State and major urban areas have adopted local solutions that are now being linked together through common standards and practices. Some of these include Los Angeles, Jacksonville, Eastern Missouri, Washington State, and San Diego. As shown in Figure 1-2, San Diego's Automated Regional Justice Information System (ARJIS) system, which has supported the local sharing environment for many years, is now linked with national information sources.

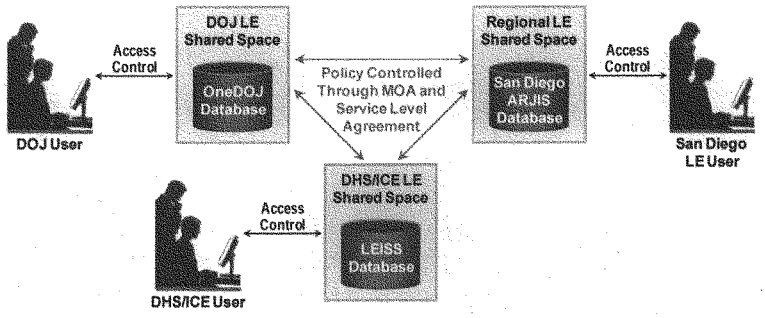


Figure 1-2. Example Law Enforcement Information Flow

With the growing success of these information sharing activities, participating agencies can now search a number of data repositories—commonly referred to as "ISE Shared Spaces"—to assist in connecting activities, trends, or patterns in their jurisdictions to those of others, significantly enhancing intelligence-led policing and terrorism-related crime reduction activities. (See Section 2 for more information on the Shared Space concept.) These efforts all achieve *national sharing* under *local control* and feature distributed architectures, common standards, collaborative governance, improved business processes, and attention to privacy concerns as envisaged and enumerated in the Presidential Guidelines. Further, these efforts leverage, enhance, and extend existing information sharing initiatives, and reflect a shared and growing culture of information sharing on the part of all participating agencies.

1.4 ISE Performance Management

1.4.1 Introduction

Developing the ISE is a continuous, evolutionary process. Effective ISE performance management provides the PM-ISE and the ISC with data to make fact-based decisions and hold agencies accountable for the ISE's evolution. Performance management practices allow the PM-ISE and the ISC to evaluate and refine information sharing policies, business processes, architectures, standards, and systems across all five ISE communities.

Based on the early stage of maturity of many ISE capabilities, performance management activities currently focus on assessing ISE progress. As such, current measures used to gauge ISE implementation progress are characterized as output or compliance measures and generally focus on the progress of individual ISC member agencies. However, as the ISE matures, the performance management approach will itself mature to move from measuring individual agency progress to measuring the overall performance of the ISE. Future measures will evolve, therefore, to emphasize the mission outcomes or results of implementing elements of the ISE. These future measures will focus on the extent to which the ISE has been implemented and sharing improved, while also measuring what has been and remains to be accomplished. This approach will enable the ISE to ultimately measure the performance of its capabilities, including those designated as Fiscal Year (FY) 2009–13 ISE investment priorities. Figure 1-3 depicts the evolution of performance management as it follows ISE maturity.

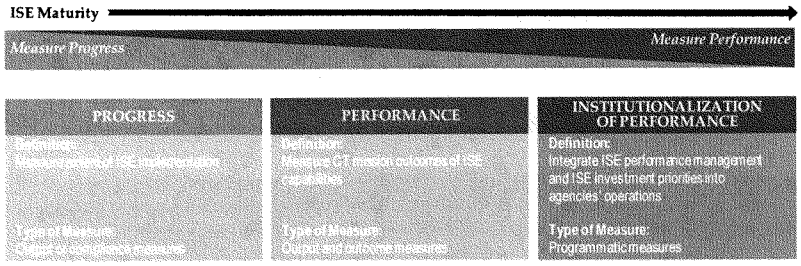


Figure 1-3. ISE Performance Management Evolves as the ISE Matures

Annual performance goals are used to measure the progress in constituting ISE capabilities. First introduced in last year's Annual Report, the four 2008 Performance Goals were designed to provide a target level of performance against which actual achievement could be compared (see Table 1-1). The goals were developed to comply with the performance management requirements of IRTPA, as well as to highlight the direction and strategies embodied in the President's Information Sharing Guidelines and Requirements. The goals are aligned with the Guidelines and Requirements report recommendations that were approved by the President in November 2006, and the data collected from ISC agencies serves to demonstrate that implementation is well underway.

Using these goals and a set of key measurement areas which assess the progress associated with each goal, the PM-ISE and ISC established an ISE baseline of performance in the fall of 2007 and measured agencies' progress against this baseline through an assessment in the spring of 2008. The fall 2007 and spring 2008 performance assessments provided the PM-ISE and the ISC with fact-based data to support decisions and report progress against key information sharing drivers, such as the Presidential Guidelines and Requirements and the NSIS.

Table 1-1. 2008 ISE Performance Goals

2008 ISE Performance Goals
Establish a set of activities and strategic approaches to facilitate sharing among all levels of government, the private sector, and foreign partners.
Develop a shared set of values that change behavior of ISE participants through established training programs, trained personnel, incentive programs, and privacy protections among ISE participants.
Establish interoperability that facilitates sharing through a common ISE Information Technology (IT) security framework, to include approved ISE wide Information Assurance (IA) solutions, government-wide physical and personnel security practices, as well as a Controlled Unclassified Information (CUI) framework across the ISE.
Establish capabilities that allow ISE participants to create and use quality terrorism-related information by improving business processes, developing a common enterprise architecture framework, refining common standards, and instituting effective resource management for government-wide programs.

1.4.2 Performance Assessment Results

The ISE agencies' self-reported baseline and spring performance data show positive accomplishments across each of the performance goals while highlighting several items that will require further attention as the ISE matures. What the ISC learned from this exercise was that very few agencies had been collecting the data needed to easily track progress against specific ISE initiatives. In addition, most had not yet incorporated meaningful information sharing measures into their own agency performance management processes.

The performance data, gathered from 15 ISC member agencies through the spring and fall assessments, is summarized below. Viewed collectively, the measures demonstrate progress against the 2008 Performance Goals. The gauges next to each measurement area below indicate both the fall baseline and spring levels of performance. As illustrated below, for some of the 2008 Performance Goals, the ISC assessed progress qualitatively but did not establish a specific measure. For these areas, the Report either details the progress made or documents a need for further action to be completed.

2008 Performance Goal: Develop a shared set of values that change behavior of ISE participants through established training programs, trained personnel, incentive programs, and privacy protections among ISE participants.

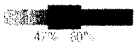
Roughly half of ISC member agencies reported that they have taken steps to meet this goal of changing behavior in the areas of training programs and personnel, incentives to share, and privacy protections.

- *Training* – In addition to the ISE Core Awareness Training [redacted] expected to be available this summer, ISE participants are required to develop tailored training programs that achieve specific, related,

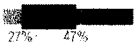
learning objectives.[12] One-third of the agencies surveyed in the fall indicated that they had established and completed some form of training to increase information sharing awareness. This number increased to 47% in the spring assessment and is expected to increase with the publication of the ISE Awareness Training Course in the summer of 2008.

- *Incentives* – Several agencies provided actual examples of how they use incentives to promote information sharing including personnel recognition, cash awards, and other rewards.[13] The overall response of agencies using information sharing incentives grew from 40% last fall to 73% in this spring's performance assessment.

- *Privacy* – Fall baseline data revealed that 47% of agencies had established privacy policies that complied with the ISE privacy guidelines, a number that increased to 60% in the spring assessment. ISE agencies' adoption of the *ISE Privacy and Civil Liberties Implementation Guide,* released in September 2007, is expected to gradually (but significantly) increase the number of privacy-compliant agencies.



- Other Elements of Creating a Culture of Sharing –
  - *Personnel Appraisals* – Last fall, ISE agencies' self-reported data revealed that 27% of ISC member agencies have taken initial steps to ensure accountability for information sharing via performance appraisals. The number grew to 47% this spring, with several agencies requesting coordination with the Office of Personnel Management (OPM) to insert information sharing into their performance appraisals. Additional agencies also reported a desire to use ISE-wide training to determine the elements needed to evaluate personnel performance in terrorism-related information sharing.



  - *Disincentives* – In the fall assessment, 53% of agencies were able to identify steps they took to remove information sharing disincentives in the areas of document dissemination (e.g., reduced use of originator controls), writing for release, and policies for sharing between internal departments. This number increased to 73% for the spring assessment.

2008 Performance Goal: Establish interoperability that facilitates sharing through a common ISE IT security framework, to include approved ISE-wide Information Assurance (IA) solutions, government-wide physical and personnel security practices, and as a CUI framework across the ISE.

[12] ISE IP, op. cit., p. 84-86.

[13] *Implementing Recommendations of the 9/11 Commission Act of 2007* (9/11 Commission Act), P.L. 110-53, Section 210, (August 3, 2007).

In line with the goal of establishing interoperability, a number of ISC member agencies demonstrated progress establishing ISE shared spaces. However, there is room for improvement in focusing ISE efforts on reducing barriers—both in shared spaces and in physical and personnel security practices as well as in moving toward a CUI framework.

- *Shared Spaces* – The *ISE Profile and Architecture Implementation Strategy (PAIS)* provides the official standard [redacted] necessary to implement ISE shared spaces was published in May 2008.[14] After close coordination with agency Chief Information Officers (CIOs), enterprise architects, and Office of Management and Budget (OMB) officials, the fall baseline response of 13% of agencies having implemented shared spaces grew to 33% in the spring.
- *CUI Framework* – As noted earlier, a policy framework has been established and released by the President for standardizing SBU (now termed CUI) information. Because the CUI framework was only recently approved (May 2008), the PM-ISE was not able to collect performance data. Section 4 provides further detail on the progress achieved.
- *Physical and Personnel Security Practices* – The ISE has begun to coordinate and collaborate on security policies across the five ISE communities. The PM-ISE did not collect performance data on this topic; however, it intends to focus efforts on this area in the future.

2008 Performance Goal: Establish a set of activities and strategic approaches to facilitate sharing among all levels of government, private sector, and foreign partners.

Considerable progress has been achieved in sharing with Federal and SLT governments, yet further data is needed to evaluate sharing with the private sector and foreign partners.

- Sharing Among All Levels of Government –
  - *ITACG* – The Interagency Threat Assessment and Coordination [redacted] Group (ITACG) has achieved 75% of its initial operating capability, specifically in the areas of staffing, establishing standard procedures, and integrating operations with the National Counterterrorism Center (NCTC).[15]

[14] Version 2.0 of the Enterprise Architecture Framework scheduled to be released in Fall 2008, will provide further detail on ISE Shared Spaces.

[15] For purpose of the Spring 2008 ISE Assessment, initial operating capability was defined as: staffed with the appropriate Federal, state, local, and tribal representatives; operating based on a finalized set of standard operating procedures (SOPs); drafted a budget to be fully funded over the next two fiscal years; reviewing Federal products to ensure that they are incorporating SLT requirements; incorporating the ITACG within DHS and FBI operations; and developing and disseminating products.

Further information on the ITACG can be found in Section 5 of this Report and in a separate Report to Congress.[16]

- *Suspicious Activity Reporting (SAR) Processes* – Roughly half (53%) of agencies reported having a Suspicious Activity Reporting (SAR) process in place. While the data made it clear that SAR processes are generally not yet standard across the ISE, the percentage of agencies that reported having a SAR process in place increased to 73% in the spring assessment.

- *Sharing with Foreign Partners* – The Foreign Government Information Sharing Working Group developed a checklist of issues for agencies to consider when negotiating terrorism-related information sharing agreements with foreign partners, including privacy protections and possible review procedures. Released this spring, the checklist was recommended but not mandatory. As part of the spring 2008 measurement findings, 13% of ISC member agencies reported having adopted the checklist in Department-wide processes.

State and Major Urban Area Fusion Centers - Both DOJ and DHS are able to document Federal activities completed in support of establishing and maintaining a baseline level of capability for fusion centers, including providing training and connectivity, and attempting to tie baseline capabilities to the grants process. Further information regarding fusion centers can be found in Section 3.

Sharing with the Private Sector – Sharing with the private sector is called for in the NSIS and remains a priority for the ISE. Though no performance data were collected at this time, efforts such as the FBI's InfraGard Program which shares information with private sector infrastructure security officials through a homepage on the LEO network, reflect progress achieved in sharing information with the private sector.

2008 Performance Goal: Establish capabilities that allow ISE participants to create and use quality terrorism information by improving business processes, developing a common enterprise architecture framework, refining common standards, and instituting effective resource management for government-wide programs.

This goal refers to the successful incorporation of information sharing into agencies' routine mission operations. Several elements have been achieved that demonstrate how the ISE agencies are beginning to account for information sharing in their operations, including enterprise architecture, CTISS, performance, and investment structures. These elements will be discussed throughout the remainder of this Report,

[16] *Report to Congress on Establishing the Interagency Threat Assessment and Coordination Group*, PM-ISE (February 2008). Available online at: http://www.ise.gov.

specifically in Sections 2 and 7. One additional element of ISE institutionalization that was tracked as a part of the baseline and spring measurement efforts was information sharing governance.

- *CTISS* –In part because of their participation in developing the ISE-SAR Functional Standard, the first Common Information Sharing Standards (CTISS) program issuance, 33% of agencies reported adoption of the CTISS Program. The number of agencies adopting the CTISS Program increased to 47% after the January 2008 release of the ISE-SAR Functional Standard, and several agencies were also adopting Agency-wide standards processes. In addition, agencies cited the NIEM and Federal Enterprise Architecture (FEA) Standards as examples of where they are working across the ISE to align technologies to facilitate information access and exchange.
- *Governance* – As a means to facilitate information sharing within their own agencies and across the environment, a full 93% of agencies reported having established their own information sharing governance bodies in the spring assessment. This is an increase from the 73% of agencies that reported having established governance bodies last fall. This measure is a positive indicator of ISE members taking steps to ensure that information sharing is appropriately addressed within their agencies.

ISE accomplishments are clear when viewed according to the Presidential guidelines and requirements. The PM-ISE, in consultation with the ISC, is implementing the guidelines by leveraging ongoing information sharing efforts and promoting a culture of information sharing. The remaining sections of this Report complement the vision for the ISE and the ISE performance management results by providing a detailed overview of ISE progress against each of the Presidential guidelines and requirements, as well as planned activities to further the ISE's evolution in the upcoming year.

2 Establishing Information Sharing Standards

"The ISE must, to the extent possible, be supported by common standards that maximize the acquisition, access, retention, production, use, management, and sharing of terrorism information within the ISE consistent with the protection of intelligence, law enforcement, protective, and military sources, methods, and activities."
— Guidelines and Requirements in Support of the ISE, Guideline 1

A smoothly functioning ISE requires the construction, integration, and sustained operation of standardized terrorism-related information sharing infrastructures across the Federal Government, SLT governments, and where appropriate, the private sector and foreign partners. A business process-driven architectural framework, buttressed by a common standards development approach, is driving ISE architecture and standards implementation by Federal agencies. This section also singles out two areas that are especially important in helping to both help remove impediments to sharing and help agencies improve sharing practices. Implementation of ISE Shared Spaces is discussed in Section 2.4, while the essential ISE attributes of trust and security are covered more fully in Section 2.5.

2.1 2007-08 Highlights

Highlights of progress this year include:

- Publication of the first version of the ISE Enterprise Architecture Framework (ISE EAF) in August 2007 and its companion ISE PAIS in May 2008;
- Formal establishment of the ISE standards program and publication of the first ISE functional standard that institutionalizes an integrated ISE SAR process;
- Development of ISE Shared Spaces to support operational exchanges of terrorism-related information;
- Demonstration of the ISE EAF and CTISS in operational pilots;
- Leveraging of the fundamental concepts of the ISE EAF and PAIS by DOJ, DHS, and others for applications broader than the ISE; and
- Development of a common ISE security risk management framework.

2.2 ISE Enterprise Architecture Framework

A major requirement of the ISE is to standardize and rationalize the inherent differences and distinct separation of information resources across the Federal Government and between Federal and SLT agencies. Systems are budgeted for and implemented by individual agencies in all ISE communities. The challenge then is to provide a unifying

construct—based on common standards and core services—that still accommodates the need for individual ("mostly common") implementations. To address this challenge, the PM-ISE established the ISE Architecture program to align and integrate the vast collection of diverse information technology systems used by all ISE participants into a more uniform, interconnected ISE-wide system of systems. Figure 2-1 depicts a top-level view of a portion of the ISE EAF demonstrating how two ISE participants would share in the ISE.

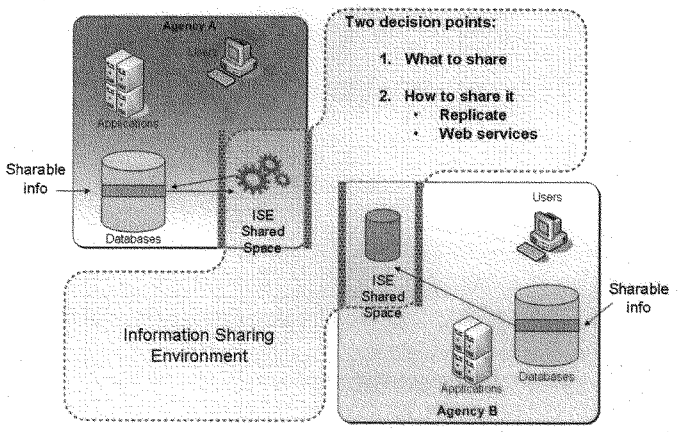


Figure 2-1. Overview of the ISE Enterprise Architecture Framework

The ISE Architecture program, employing cross-governmental working groups such as the Chief Architects' Roundtable, continues to make progress in addressing this technology challenge. Specific accomplishments include:

- In August 2007, the PM-ISE released the first version of the ISE EAF, a strategic guide for mapping ISE participants' enterprise architectures into the Government's FEA. The ISE EAF provides a roadmap to enable long-term, institutionalized technology improvement and information systems planning, investing, and integration to support the sharing of terrorism-related information and identifies the network interfaces and standards needed to facilitate information sharing.
- In May 2008, the PM-ISE released the first PAIS document to help guide ISE Federal agencies with near-term implementation efforts to interconnect information resources; make these resources readily available; and access other data, networks, and services provided by the ISE. The Federal CIO Council's Architecture and Infrastructure Committee and OMB reviewed and approved the PAIS as a valid document to guide information sharing requirements.

2.3 Common Terrorism Information Sharing Standards

The need for ISE standards is cited in thirteen separate places in the NSIS—an explicit recognition that common standards are the fundamental building blocks enabling effective and efficient information sharing. As a result, the PM-ISE has worked with the ISC and SLT governments to develop and implement standards to improve the operation of ISE business processes and implement compatible technology capabilities in ISE participants' networks and supporting infrastructure. The CTISS program integrates information exchange standards, based on common ISE business processes and developed through the DOJ and DHS NIEM program management office, into new ISE-wide functional standards. NIEM epitomizes a successful Federal, State, local, tribal, and private sector initiative and provides a foundation for nationwide information exchanges leveraging data exchange standards efforts successfully implemented by the Global Justice Information Sharing Initiative. NIEM is also being strongly embraced by the private sector technology community. Being part of the ISE EAF and supported by NIEM, the CTISS program is also compliant with the Federal Enterprise Architecture's Data Reference Model, a standards-based model designed to optimize data architectures to help enable information sharing and reuse across federal agencies.

- In October 2007, the PM-ISE formally established the CTISS program. CTISS standards are business process-driven, performance-based "common standards" for preparing terrorism information for maximum distribution and access within the ISE. The CTISS Committee, a subcommittee under the ISC, now provides ongoing governance, configuration management, and cross-agency, cross-government CTISS coordination and review.
- In January 2008, the PM-ISE issued the first CTISS functional standard that provides the data and information sharing foundation for operational information sharing of SARs in the ISE and supports demonstrations to include the SAR Evaluation Environments and an effort by the Los Angeles Police Department (LAPD) to redefine its terrorism SAR policies and processes.
- DOJ and FBI are already working with fusion centers to adopt and implement the SAR functional standard at the Federal level and at selected fusion centers. The Department of State also has a project underway to apply the standard to its SAR database.
- The PM-ISE also identified initial technical standards supporting information assurance and transport to ISE infrastructure assets, and will also actively work with all agencies, including the Department of Defense

In part because of their participation in developing the ISE-SAR Functional Standard, 33% of agencies reported adoption of the CTISS Program. The number of agencies adopting the CTISS Program increased to 47% after the January 2008 release of the ISE-SAR Functional Standard, and several agencies were also adopting agency-wide standards processes.

participants are assured that the information they provide will be adequately protected;

- Is integrated with the ISE EAF and PAIS; and
- Employs information security standards and guidance developed by the National Institute for Standards and Technology (NIST), and builds on the foundation of trust between the defense and intelligence communities.

Figure 2-2 shows the specific activities in the ISE Risk Management Framework and the NIST security standards and guidelines associated with each activity.

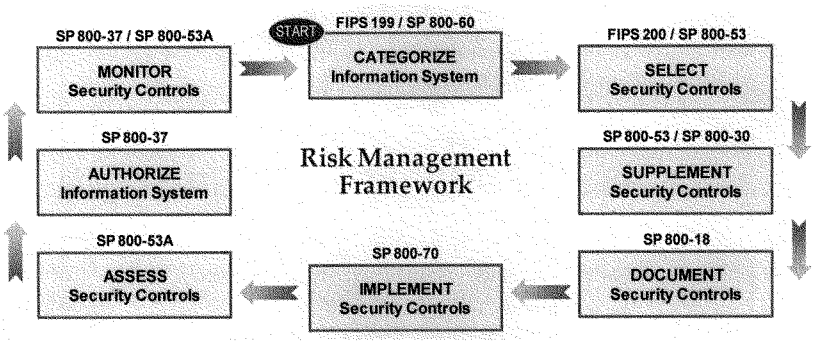


Figure 2-2. The ISE Risk Management Framework

2.5.2 Improved Security Practices

Cumbersome personnel and IT security processes seriously inhibit efficient exchange of terrorist-related information. ISE success ultimately depends on streamlining the granting and mutual recognition of security clearances and IT system accreditations.

- The PM-ISE and ISC are leveraging a joint DoD and DNI CIO effort to drastically streamline the Certification and Accreditation (C&A) process for national security systems. DoD and the Office of the DNI (ODNI) have updated the ISC to ensure that other agencies are aware of the standards and processes they have developed by the ODNI and DoD. The aim is to use using a mostly common set of standards to guide C&A activities across the ISE and achieve reciprocity wherever possible (see the "Authorize block" in Figure 2-2).

The C&A process is used by Federal agencies and others to determine if an information system is approved for operation. Certification involves an evaluation of the technical and non-technical security features of the system. Accreditation is a formal management decision—using certification results as input—that a system is approved to operate at an acceptable level of risk.

- NCTC Online, a web-based capability that now allows State and major urban area fusion centers to access Secret national terrorism-related information; and
- Law enforcement information shared by DOJ and ICE, a component of DHS, through LEO and RISSNET.

The PAIS provides the official standard necessary to implement ISE shared spaces. After close coordination with agency CIOs, enterprise architects, and OMB officials, the fall baseline response of 13% of agencies having implemented shared spaces grew to 33% in the spring, as further guidance was made available to agencies.

In these and other cases, the essential point is that such infrastructure elements interconnect and make terrorism-related information accessible to all authorized ISE participants. By FY 2010 agencies participating in the ISE are expected to build on existing or planned information technology resources to create ISE Shared Spaces to support the national CT mission.[17]

2.5 Building a Trusted Environment

The concept of trust is fundamental to the ISE. Seven of the 15 ISE attributes identified in IRTPA deal with aspects of trust or security.[18] The NSIS refers to the terms "trust" or "trusted" at least ten times, calling for the need to "enable the trusted, secure, and appropriate exchange of terrorism-related information ... at all levels of security classification." Increased sharing depends on ISE participants' trust that recipient organizations will adequately protect the information against unauthorized disclosure or other misuse. In the last year, Federal agencies have developed a common ISE risk management framework and made strides in improving security practices.

2.5.1 ISE Risk Management Framework

The basis for achieving trust in the ISE is adoption of a common risk management and information security framework to allow officials in all five ISE communities to make the appropriate tradeoffs between sharing and protection and lead eventually to mutual acceptance of security assessments. The risk management framework:

- Embodies the basic principles of information security—confidentiality, integrity, and availability—so that ISE

The FBINET pilot project addresses personnel, facility, and IT requirements for installation of a Secret level capability at a fusion center. In a practical example of risk management, the FBI modified its security requirements which differed from those of DHS to better address fusion centers' needs. More importantly, FBI and DHS are working to harmonize their security requirements for fusion centers so that there will be only one standard for installation and operation of Secret domain networks.

[17] Additional guidance on implementing shared spaces will be provided in Version 2 of the ISE EAF.
[18] IRTPA, as amended, op. cit., §1016(b)(2)(A-O).

participants are assured that the information they provide will be adequately protected;

- Is integrated with the ISE EAF and PAIS; and
- Employs information security standards and guidance developed by the National Institute for Standards and Technology (NIST), and builds on the foundation of trust between the defense and intelligence communities.

Figure 2-2 shows the specific activities in the ISE Risk Management Framework and the NIST security standards and guidelines associated with each activity.

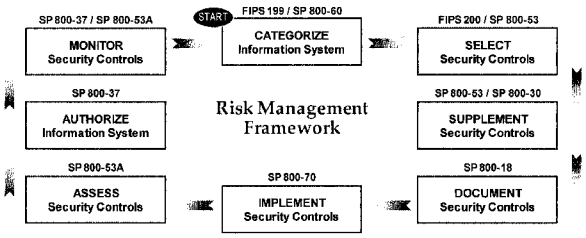


Figure 2-2. The ISE Risk Management Framework

2.5.2 Improved Security Practices

Cumbersome personnel and IT security processes seriously inhibit efficient exchange of terrorist-related information. ISE success ultimately depends on streamlining the granting and mutual recognition of security clearances and IT system accreditations.

- The PM-ISE and ISC are leveraging a joint DoD and DNI CIO effort to drastically streamline the Certification and Accreditation (C&A) process for national security systems. DoD and the Office of the DNI (ODNI) have updated the ISC to ensure that other agencies are aware of the standards and processes they have developed by the ODNI and DoD. The aim is to use using a mostly common set of standards to guide C&A activities across the ISE and achieve reciprocity wherever possible (see the "Authorize block" in Figure 2-2).

The C&A process is used by Federal agencies and others to determine if an information system is approved for operation. Certification involves an evaluation of the technical and non-technical security features of the system. Accreditation is a formal management decision – using certification results as input – that a system is approved to operate at an acceptable level of risk.

- Recommendations for transforming the security clearance process made by an interagency Joint Security and Suitability Reform Team are currently under review. Responding to a February Presidential directive, the team recommends making the clearance process faster, more reliable and reciprocal among all agencies. Planned features include:
  - An automated records-checking system using government and commercial electronic databases to replace some manual investigations;
  - A continuous evaluation program, using frequent automated record checks of cleared employees, to replace the current practice of reinvestigations every five or ten years;
  - A new electronic application that would collect security-related information, including electronic fingerprints, early in the clearance process, reduce errors and speed processing; and
  - Consolidated oversight by the DNI of the security clearance process for all levels of security classification.

2.6 Broader Application of ISE EAF and CTISS

The ISE EAF, PAIS, and CTISS provide guidance to help agencies implement information sharing capabilities, connect to other ISE participants, make information available through ISE Shared Spaces, and access ISE information and services. Because they break new ground in several areas, however, they have had unexpected spin-offs beyond the bounds of the ISE. There are many success stories both inside and outside the ISE resulting from the CTISS effort to leverage NIEM and DoD-DNI UCORE data standards to facilitate information exchanges between different domains or communities of interest.

DHS, for example, is using guidance from the ISE EAF with NIEM to construct almost 50 reusable information exchanges across the full range of its mission areas. The DHS Regional Sharing Service initiative has also deployed information sharing technologies and operating policies in compliance with the ISE EAF supporting information sharing between ICE and local law enforcement agencies in Seattle, WA, Laredo, TX, and Los Angeles, CA. DHS is further using NIEM to develop the next version of the Common Alerting Protocol, a simple, general format for exchanging all-hazard emergency alerts and public warnings over different networks. This capability provides valuable analytic inputs into the ISE-SAR and alerts, warnings, and notifications (AWN) processes with emerging patterns derived from local warnings that might indicate undetected hostile acts. The Domestic Nuclear Detection Office, in coordination with DHS/Customs and Border Patrol, is providing NIEM-based information exchanges with State and local entities, to include those now participating in an interstate radiation detection information sharing effort—the Southeast Transportation Corridor Pilot Program. NIEM is also developing a standard for interoperability between Emergency Operations

Centers in a number of State and local communities that will be an important part of connectivity efforts between collocated fusion centers and the ISE.

DOJ is taking a similar approach, building information sharing segment architectures leveraging concepts from the ISE EAF, with a focus on State and local law enforcement sharing through capabilities such as the N-DEx, supported by LEO, RISS, and the National Law Enforcement Telecommunications System, a state owned system connecting all 50 states and territories along with every federal agency with a Justice component. N-DEx, activated by the FBI in March 2008, currently incorporates data from Oregon, Delaware, Nebraska, and the Oneida Nation with additional SLT participants' information added in the coming months. The PM-ISE is also working closely with the FBI SENTINEL program management office in developing the case management system to be NIEM-conformant to be able to exchange information with ISE systems and processes.

Individual states—including Florida, New York, Texas, and California—are also using NIEM and ISE guidance to drive SAR implementation. The state of Florida is using NIEM for all law enforcement information exchanges between over 453 law enforcement agencies coordinating among eight (seven regional and one State) fusion centers. Fusion Centers in other states are also incorporating NIEM requirements into their information technology procurements, and other ISC member organizations are in varying stages of adopting the same approaches. In one of the more interesting spin-offs, the national health care community is considering leveraging ISE EAF and CTISS concepts to help meet its national health information sharing needs.

2.7 Next Steps

2.7.1 Architecture and Standards

As the PM-ISE and ISC continue to implement terrorism-related information sharing architectures and business process-driven, common standards across the ISE, they must continue to mature the ISE EAF and PAIS and increase the inventory of common standards. Since the role of the PM-ISE is to *plan for and oversee* the implementation of the ISE, actual implementation is the responsibility of Federal agencies. To ensure that this implementation is consistent with the ISE EAF and CTISS, the PM-ISE must leverage the alignment and integration of performance management and investment strategies to institutionalize these infrastructures (see section 7). The primary activity here is to continue to transition architectural guidance and standards back into the Federal Enterprise Architecture. Planned activities include the following:

- Publishing Version 2 of the ISE EAF and ISE PAIS to incorporate additional terrorist watchlist and AWN mission business processes;
- Continuing to identify those processes that will benefit from a functional standard and assigning the necessary resources to develop the business process maps,

information flow descriptions, and data elements that are essential parts of any ISE functional standard;

- Assisting OMB in overseeing implementation of the ISE EAF, Shared Space, and CTISS and related information sharing functional and technical standards through regular reviews of agency Enterprise Architectures and related investment plans;

2.7.2 Building a Trusted ISE

Trust and security will continue to be important considerations for the ISE. 2008-09 plans include:

- Leveraging a joint DoD and DNI CIO effort to streamline departmental C&A processes. Achieve C&A reciprocity between ISC members to the maximum extent possible;
- Aligning policies to guide sharing across multiple security domains by accrediting and deploying at least one solution identified by or developed through the Unified Cross Domain Management Office; and
- Extend the ISE risk management framework to all ISE stakeholders, especially SLT governments and the private sector where appropriate. The PM-ISE and the ISC will build on the ISE Trusted Broker pilot by fielding a limited capability to provide improved access and identity management.

3 Sharing Within, Across, and Between Levels of Government

"Recognizing that the war on terror must be a national effort, State, local, and tribal governments, law enforcement agencies, and the private sector must have the opportunity to participate as full partners in the ISE..."

— Guidelines and Requirements in Support of the ISE, Guideline 2

Combating terrorism is a national mission that requires cooperation at all levels of government and the private sector. The Guideline 2 framework, approved in November 2006, provides the foundation for a variety of activities, described more fully below, that strengthen the ties nationally among agencies with a CT mission.

Critical components of improved sharing are ISE business processes that remove traditional impediments to sharing and streamline the ways in which agencies exchange information. This section outlines progress in critical ISE processes for SAR, terrorist watchlists, and AWN.

3.1 2007-08 Highlights

Highlights of the effort to improve sharing within, across, and between Levels of Government include:

- Establishing the ITACG and initiating development of an integrated network of fusion centers to enable the effective sharing of terrorism-related information between Federal and SLT partners;
- Providing common tools and mechanisms that assist agencies in facilitating the sharing of terrorism information with foreign governments;
- Working with fusion centers and local law enforcement departments to integrate a standard ISE-SAR business process into the day-to-day operational environments of their region; and
- Evaluating terrorist watchlist and AWN business practices to rationalize, standardize, and simplify them within the ISE.

One example of improving sharing practices in the Federal government is the FBI's initiative to equip field agents with personal digital assistants (PDAs) to provide wireless access to a wide range of SBU level terrorist-related information, including watchlists. As the result of a successful pilot effort, the bureau is now deploying 19,500 PDAs to more than 56 field offices.

3.2 Sharing Information with State, Local, and Tribal Governments

As referenced in the NSIS, the national information sharing framework for sharing with SLT governments has two primary objectives:[19]

- Ensuring the Federal Government provides information in ways that better meet the needs of SLT partners through the establishment of an ITACG within the NCTC. This integrated approach allows Federal agencies to work together to disseminate a federally-validated perspective on available threat information.[20]
- Supporting improved collaboration at the State and local levels by designating fusion centers "as the primary focal points within the State and local environment for the receipt and sharing of terrorism-related information" and by establishing and sustaining a national integrated network of these centers.[21]

In July 2007, Congress passed the 9/11 Act which statutorily created the ITACG and designated the PM-ISE "to monitor and assess" its efficacy.[22] The Act also called for a DHS State, Local, and Regional Fusion Center Initiative which, among other requirements, must "support efforts to include State, local, and regional fusion centers into efforts to establish an information sharing environment."[23] The NSIS further advanced these initiatives by providing a detailed description of the role of the ITACG and the roles and responsibilities of Federal and SLT governments. In the past year, significant advances have been made in implementing the NSIS objectives.

3.2.1 The Interagency Threat Assessment and Coordination Group

As required by the 9/11 Act, the PM-ISE submitted a *Report to Congress on Establishing the Interagency Threat Assessment and Coordination Group* which details the progress achieved in establishing the ITACG as of early February. In summary, the ITACG achieved initial operating capability in the areas of staffing, establishing standard procedures, and integrating operations with the NCTC, though more remains to be done before the ITACG can be considered fully operational. Both DOJ and DHS are able to document Federal activities completed in support of establishing and maintaining a baseline level of capability for fusion centers, including providing training and connectivity, and attempting to tie baseline capabilities to the grants process. Since the Report was issued, the ITACG Advisory Council met in April and June 2008, focusing on recruitment for next year's detailees; and agreeing to a Concept of Operations for a Detailee Fellowship Program. The full report is available at www.ise.gov.

[19] NSIS, op. cit., p. 30.
[20] Ibid., p.18.
[21] Ibid., p.20.
[22] 9/11 Commission Act, §521(c), op cit. The ITACG was established as part of the ISE IP and Guideline 2, but the statute strengthened several of its functions and provided for additional oversight.
[23] Ibid., § 511(b)(2).

3.2.2 State and Major Urban Area Fusion Centers

Today, there are over 60 operational fusion centers in 48 states. In most states with multiple fusion centers, Governors have designated a single fusion center to coordinate statewide information sharing efforts with the Federal Government. The interagency National Fusion Center Coordination Group (NFCCG), co-chaired by DHS and the FBI, is responsible for ensuring that the Federal Government's efforts to work with fusion centers are coordinated and carried out in a manner consistent with the NSIS.

To further these coordination efforts, the Federal Government is asking that fusion centers achieve and sustain a baseline level of capability and establish electronic connections with the Federal Government and each other. The NSIS goal is an integrated network of fusion centers to enable the effective sharing of terrorism-related information.[24] The Federal Government is developing Baseline Operational Capability Standards for fusion centers to ensure that they have the necessary structures, standards, and tools in place to support the gathering, processing, analysis, and dissemination of terrorism-related information.[25] Once achieved, national baseline capabilities will provide a forum from which fusion centers can support specific operational capabilities such as SAR, AWN, statewide or regional risk assessments, and situational awareness reporting.

Where current Federal support efforts are underway, a sustained Federal partnership with fusion centers is critical. Efforts to build this partnership include:

- *Planning*. A Federal Coordinated Support Plan is under development by DHS, FBI, and other Federal agencies to support the establishment and sustainment of this baseline capability through *technical assistance and training, human support*, and *connectivity*.
- *Technical Assistance and Training*. The DHS/DOJ Fusion Process Technical Assistance Program is assisting fusion centers in achieving baseline capabilities by providing training and technical assistance on such topics as governance, fusion center management, and privacy policy. The Federal Government is supporting an assessment of fusion center

This year, fusion centers provided intelligence used in over 50 DHS Homeland Intelligence Reports (HIR). In March 2008, a DHS HIR from Ohio was used as a source for an article in the Presidential Daily Brief. This is a prime example of how personnel assigned to fusion centers are helping to facilitate the movement of information from state to senior-level Federal authorities.

[24] NSIS, op. cit., pp. 14 and A1-3.

[25] This document is being constructed based on the fusion process capabilities outlined in the 2007 Fusion Center Assessment and the 2007 and 2008 Homeland Security Grant Program Fusion Capability Planning Tool Supplemental Resource. The baseline operational standards are being developed using guidance provided in the following national policy documents: the *Fusion Center Guidelines*, the *National Criminal Intelligence Sharing Plan*, the *Information Sharing Environment Implementation Plan*, and the U.S. Department of Homeland Security's National Preparedness Guidelines and Target Capabilities List.

capabilities, identifying and documenting capability gaps, and developing a strategy and investment plan to mitigate these gaps. Training and technical assistance priorities include improving fusion center analysis and incorporating other disciplines—fire, public health, etc.—into fusion center operations. As of May 2008, 96 technical assistance services had been provided to jurisdictions, and additional technical assistance continues to be available upon request.

- *Human Support.* The Fusion Center Initiative also deploys personnel to assist fusion centers in blending law enforcement and intelligence information analyses and coordinating security measures to reduce threats in local communities. DHS and FBI have deployed over 200 people to fusion centers thus far. This number is expected to grow as part of a coordinated interagency approach that supports the assignment of Federal personnel to fusion centers and strives to integrate and, to the extent practicable, co-locate resources.
- *Connectivity*: Significant progress has been made to provide fusion centers with protected access to Secret and Unclassified Federal systems including direct access to NCTC on line at the Secret level via multiple paths such as FBINET, the DoD Secret Internet Protocol Router Network (SIPRNET), and the Homeland Security Data Network (HSDN). Both DHS and FBI have amended their security policies so that they are consistent across FBINET and HSDN. Access to RISS, LEO, and the Homeland Security Information Network (HSIN) allow users at all fusion centers to communicate and exchange information at the SBU/CUI level. At the Secret level, 16 fusion centers are connected to DHS' HSDN Network and 27 have FBINET connectivity. By the end of 2008, 41 fusion centers will be connected to HSDN and 46 to FBINET.

3.2.3 Tribal Governments

Tribal governments play an important role in our efforts to foster a coordinated SLT information sharing network. In 2006, the ISE and the Department of the Interior initiated the Tribal Nations Information Sharing Pilot Project (TN-ISPP). During 2007, the Project assessed the information sharing needs of four federally recognized tribes whose reservations were located on or near international borders: the Tohono O'odham Nation (Arizona), the Cocopah Tribe (Arizona), the Blackfeet Tribe (Montana), and the Sault Ste. Marie Tribe (Michigan). After the assessments were conducted and prior to TN-ISPP completion in March 2008, equipment was purchased and installed at Blackfeet and Cocopah, which will greatly enhance the ability of those two tribes to better support NSIS requirements. Efforts are also ongoing to explore how best to integrate tribal representation at fusion centers.

3.3 Sharing Information with the Private Sector

As noted in last year's Annual Report, the PM-ISE and ISC agreed in January 2007 to leverage the nation's Critical Infrastructure and Key Resources (CI/KR) sector partnership structure, as defined in the National Infrastructure Protection Plan (NIPP)

and managed through DHS, as the primary private sector coordination mechanism for the ISE. The CI/KR Sector Partnership includes:

- CI/KR owners or operators and trade associations representative of CI/KR owners and/or operators;
- Government agencies and officials relevant to their CI/KR infrastructure protection mission interests; and
- Subject-matter experts upon whom they depend to support infrastructure protection mission activities.

Defined in the NIPP, the partnership includes the 17 CI/KR sectors identified within Homeland Security Presidential Directive 7 (with one additional CI/KR sector created by DHS) along with the cross-sector councils supporting the sector's critical infrastructure protection activities.

DHS is equipping state police flight crews with a cutting-edge aerial technology. Piloted with the Maryland State Police (MSP) Aviation Command, the new technology—known as the Critical Infrastructure Inspection Management System (CIIMS)—helps state police to efficiently manage inspections of critical structures, such as dams, bridges, and large industrial complexes. Before the CIIMS technology was available, MSP flight crews relied upon paper files to document inspections. Nationally replicable, CIIMS provides flight crews with an easy-to-use, tablet-sized computer equipped with touch-screen controls that aid data collection efforts and expedite information sharing among local, State, and Federal agencies.

The CI/KR information sharing environment is being implemented through the development of information sharing policies and the coordinated development of core and enhanced mission-related information sharing processes. It will support three levels of decision-making and action: (1) strategic planning and investment; (2) situational awareness and preparedness; and (3) operational planning and response.[26]

In addition, the FBI InfraGard program is a government and private sector alliance comprised of CI/KR stakeholders from the Federal and SLT governments as well as the private sector. As of February 2008, the number of InfraGard members increased to 24,000 in 86 chapters nationwide. Members have access to InfraGard's secure website on the LEO network infrastructure through which they receive information and CI/KR-related intelligence products at the SBU, Law Enforcement Sensitive (LES), and For Official Use Only levels.

3.4 Improving ISE Business Processes

In this section we describe activities underway to improve and standardize business processes and rules governing suspicious activity reporting; terrorist watch lists; and AWN. The PM-ISE and ISC have been working to define important "to be" business

[26] *The CI/KR Information Sharing Environment*, Department of Homeland Security, Office of Infrastructure Protection (April 2007).

processes to improve the way terrorism-related information is shared and to drive improvements in agency architectures through the ISE EAF and CTISS.

3.4.1 Suspicious Activity Reporting

Law enforcement agencies have long relied on tips and leads about suspicious activity provided by the public and others to support anti-crime efforts. In the post 9/11 world, some of these tips and leads could potentially provide critical information regarding suspicious activities related to terrorist threats. Our challenge is to integrate terrorism-related SARs broadly in the ISE to establish "a unified process to support the reporting, tracking, processing, storage, and retrieval of ... [suspicious activity] information" while ensuring that the effort is carried out in a manner that protects privacy and other legal rights."[27]

This year, the LAPD established a department-wide process for gathering, processing, and sharing terrorism-related SARs. Consistent with the ISE-SAR Functional Standard, this process uses e-learning and roll call training to inform officers how to recognize potential terrorist activities while providing standardized reporting codes that facilitate the reporting and review of terrorism related suspicious incidents. LAPD is blending suspicious activity reports with other critical infrastructure and relevant crime data in order to identify patterns and trends that may be indicators of potential threats to locations within the city. LAPD SARs will be shared with analysts at the Joint Regional Intelligence Center and blended with information from other jurisdictions so that patterns and trends can be evaluated on a regional basis. DOJ and the Major Cities Chiefs Association are working together to use the LAPD process as a model that can be replicated in other cities.

Building on the foundational work and top level ISE-SAR business process description completed last year, there is substantial progress toward achieving this goal. The ISE-SAR Functional Standard, issued by the PM-ISE in January 2008:

- Requires all departments or agencies that possess or use terrorism or homeland security information or operate systems that support or interface with the ISE to follow a common format for sharing SAR information;
- Outlines a set of general criteria to assist operators or analysts in determining whether or not a particular report meets the threshold for designation as an ISE-SAR, i.e., one with a potential terrorism nexus; and

Roughly half (53%) of agencies reported having a SAR process in place. While the data shows that SAR processes are not yet standard across the ISE, the percentage of agencies that reported having a SAR process in place increased to 73% in the spring assessment

[27] NSIS, op. cit., (October 2007), pp. A1-6 and A1-7.

- Describes the ISE-SAR information flow, highlighting the filtering and decision-making steps that separate terrorism-related SARs from the large volume of unrelated information.

As called for in the NSIS, and building on the ISE-SAR functional standard, efforts are underway to pilot and establish a national capacity for gathering, documenting, processing, analyzing and sharing terrorism related SARs.

As an initial step, the DOJ, DHS, DoD, and the FBI, working in partnership with State and local officials, will institute a standardized approach to gathering, documenting, processing, analyzing and sharing terrorism-related suspicious activities reports. Front line law enforcement personnel will be trained to recognize behaviors and incidents indicative of criminal activity associated with domestic and international terrorism. Once documented, SARs will be evaluated by trained personnel to determine if they have a terrorism nexus. If a terrorism nexus is established, the SAR will be made available to the local JTTF, regional and/or statewide fusion centers, and DHS.

Technical resources are being provided to enable the "posting" of terrorism-related SARs to a "shared space" in a manner consistent with technical standards contained within the *ISE SAR Functional Standard* and its associated SAR Information Exchange Package Document. This will allow SARs to be accessed by fusion centers, DHS Headquarters, and JTTFs to support regional and/or national analysis. Access to the "shared spaces" will be via LEO, RISSNET and HSIN.

Protecting the information privacy and legal rights of Americans is a top priority: At the local level, SARs will be incorporated into existing processes and systems used to manage other crime-related information and criminal intelligence so as to leverage existing policies and protocols utilized to protect the information privacy, civil liberties, and other legal rights of the general public. Multiple levels of review and vetting will be established to ensure that information is legally gathered and managed, and reports containing personally identifiable information that are unfounded, or that cannot be reasonably associated with criminal activity, will not be shared beyond the originating entity.

The ISE Privacy Guidelines Committee's (PGC's) Legal Issues Working Group has completed an initial privacy and civil liberties review of the *ISE SAR Functional Standard* and its implementation. The PGC will monitor this effort, provide advice and guidance to the project teams, and issue a public report regarding privacy and civil liberties issues pertaining to this effort.

The results of this initial phase of the ISE SAR pilot will be documented to support the development and publication of an implementation guide and template for use by other state and local jurisdictions. The International Association of Chiefs of Police (IACP), the Major Cities Police Chiefs Association, Major County Sheriffs, and the Criminal Intelligence Coordinating Council (CICC) have been involved in planning and will be major players in implementation.

3.4.2 Terrorist Watch Lists

One of the most important weapons in the fight against terrorism is the U.S. Government's consolidated terrorist watchlist—the authoritative source for information on all known and appropriately suspected terrorists. The list is used by Federal and SLT agencies—including officers on the street—as well as selected foreign and private sector partners to identify and screen terrorists. An accurate terrorist watchlist, shared across the ISE, contributes both to safeguarding our nation's borders and controlling terrorist movements within the country.

The TSC has taken important steps to ensure that watchlists are accurate, standardized, and complete and that appropriate processes are in place to address Congressional direction that "all terrorism watch lists are available for combined searching in real time through the ISE and [that] there are consistent standards for placing individuals on, and removing individuals from, the watch lists, including the availability of processes for correcting errors."[28] Most recently, the TSC has:

- Established a proactive mechanism—the Terrorist Encounter Review Process—to review watchlist data related to frequently encountered individuals and make corrections or enhancements to the watchlist as appropriate;
- Expanded its efforts to ensure the quality of watchlist data by increasing the number of staff assigned to data quality management and improving quality assurance processes;
- Performed selected scrubs of watchlist data, including a special quality assurance review of the No Fly List and an ongoing record-by-record review of the entire Terrorist Screening Database (TSDB);
- Established a process and a separate office to address complaints filed by persons seeking relief from adverse effects of related terrorist watchlist screening;
- Established an interagency working group to review and implement watchlist improvement opportunities; and
- Reached out to State and major urban area fusion centers and Joint Terrorism Task Forces to help them better understand the role of the TSC and use the TSDB more effectively.

Building on TSC existing business processes, the PM-ISE is currently identifying any significant watchlist screening and information sharing gaps with implications for the ISE and making recommendations for updates to those processes as appropriate. To date, the team has:

[28] IRTPA as amended, op. cit., §1016(h)(2)(E).

- Developed a high-level, unclassified end-to-end business process and information flow from terrorist watch list nomination through the identification of information in the TSDB;
- Documented information flows for critical sub-processes including *Nomination* (includes export), *Encounter Management* (includes screening), *Redress* (includes updates to TSDB), and *General Quality Assurance*;
- Identified opportunities for improved use of the terrorist watchlist process in the ISE, to include possible development of an ISE functional standard; and
- In partnership with the TSC, DHS and NCTC worked to determine areas for improved alignment between the ISE-SAR Functional Standard and the Terrorist Watchlist Personal Data Exchange Standard (TWPDES 1.2b) in support of the *Encounter Management* process.

3.4.3 Terrorism-Related Alerts, Warnings, and Notifications

The ability of participants to generate, disseminate, and receive AWNs of potential or impending terrorist activities in near-real time is a fundamental ISE capability. The NSIS requires that the Federal Government, in coordination with SLT partners, establish processes to manage the issuance of AWNs to fusion centers regarding time sensitive threats and other information requiring some type of State or local response.[29]

Terrorist-related AWNs are produced by agencies at all levels of government—some in response to explicit statutory or regulatory requirements. They take several forms and may be disseminated through different distribution channels. Unlike the case with SAR, where the national strategic direction was to establish a unified ISE-SAR process, the situation with AWN is more complex. The goal is to rationalize, standardize, and simplify the multiple existing AWN processes that are either part of the ISE or interface with the environment in some way. As a first step, the PM-ISE and the ISC have been working to better understand the multiple "as is" processes before developing the longer term vision of how the ISE AWN process should operate. The following is the current status:

- There is general agreement on an initial working definition for AWN and development is underway of a top level analysis of the existing AWN business processes and information flows focusing on the key Federal AWN producers;
- There is now baseline information from ISC members concerning terrorism-related AWNs they produce or receive; and
- Preliminary descriptions exist for how two of the primary ISE AWN producers—NCTC and DHS—currently develop and disseminate AWN information.

[29] NSIS, op. cit., p. A1-7. The NSIS discusses AWN separate from what it refers to as "Situational Awareness Reporting," but since the same policies, processes, and applied technologies support both capabilities, we consider the two to be part of one ISE business process.

3.5 Terrorist-Related WMD Information in the ISE

The 9/11 Act amended the definition of "terrorism information" in Section 1016 of IRTPA to specifically include weapons of mass destruction (WMD) information "that could be used by a terrorist or a terrorist organization against the United States." The PM-ISE, in coordination with the ISC and with Intelligence Community (IC) and non-IC partners, has begun to document how terrorist-related WMD information is incorporated into the ISE by examining information flows across the Federal Government and from the Federal Government to SLT partners. The aim is to build upon ongoing efforts to improve the sharing of terrorist-related WMD (WMD-T) information. These efforts provide a solid foundation for improved sharing within (and outside) the WMD Community. Initiatives, to be developed in collaboration with the existing WMD information sharing community, include:

- Establishment of electronic communities of interest that provide the counterproliferation (CP) and CT communities with a common electronic workspace to address WMD-T and the CP-CT nexus issues;
- Coordination between members of the IC and non-IC partners (e.g., Inter-and Intra-agency steering, coordination, and working groups) on issues related to CP, WMD-T and the CP-CT nexus; and
- Production of tri-seal WMD terrorism threat briefings by DHS, FBI, and NCTC to ensure that SLT partners receive coordinated, accurate WMD information regardless of the source.

3.6 Next Steps

Information sharing will continue to mature as strong partnerships with Federal agencies, SLT authorities, private sector organizations, and foreign partners and allies are established and enhanced.

3.6.1 Sharing Information with SLT Governments and the Private Sector

Moving forward, the Federal Government will meet the needs of SLT partners by disseminating a federally-validated perspective on available threat information through the ITACG/NCTC and by supporting the establishment and sustainment of a national integrated network of fusion centers. Planned activities include the following:

- A fully-functional ITACG with increasing impact; and
- An approach to ensure the achievement and sustainment of a baseline-level of capability at designated State and major urban area fusion centers through:
  - Developing and maintaining a Coordinated Federal Support Plan that describes Federal Government-provided technical assistance and training, personnel support, and connectivity to State and major urban area fusion centers.

- Ensuring that, by the end of 2009, all designated statewide fusion centers that can support Secret-domain information systems have appropriate access to Secret and unclassified Federal systems that share terrorism-related information, to include direct access to NCTC on line via multiple paths including FBINET, SIPRNET, and HSDN.
- Developing a national investment strategy to sustain fusion center operations, including a delineation of current and recommended future Federal and non-Federal costs.

3.6.2 Suspicious Activity Reporting

The issuance of the ISE-SAR Functional Standard provides a solid foundation on which to build a national SAR process. Planned activities include the following:

- Revising the ISE-SAR Functional Standard and selection criteria as necessary, based on results analyzed from the ISE-SAR evaluation environments;
- Identifying and implementing lessons learned at the Federal, SLT levels from the SAR evaluation environments and replicate best practices, as appropriate;
- Periodically assessing the ISE-SAR Functional Standard and make adjustments as necessary to ensure that privacy rights are rigorously guarded; and
- Monitoring Federal agencies as they take the steps necessary to implement the ISE-SAR Functional Standard, including resource allocation adjustments where necessary.

3.6.3 Terrorist Watchlists

As with any process, attaining continuous improvement will require a broad and deep understanding of the terrorist watchlist processes involved, stakeholder needs, capabilities and limitations of technology, and collaboration and coordination among all parties involved. In the next year, the TSC will:

- Improve the accuracy and completeness of the terrorist watchlisting process; and
- Provide accurate and timely information from the TSC to all screening agencies.

3.6.4 Alerts, Warnings, and Notifications

Work is under way to ensure that all appropriate Federal entities with a potential role in AWN have been identified and to determine any outstanding Federal, SLT AWN needs. In the next year, the PM-ISE and the ISC will rationalize, standardize, and simplify the ways AWNs are handled in the ISC by:

- Identifying issues and impediments to the efficient and effective flow of terrorism-related AWN information between the Federal and SLT governments and the

private sector. This work will also include identification of the types of AWN information products SLT governments require and preferred formats and delivery methods; and

- Completing a baseline categorization of existing terrorism-related AWN information flows. Once this baseline is complete, develop an approach and actions to close identified gaps.

3.6.5 Terrorist-Related WMD Information

ISC agencies will collectively evaluate existing WMD information sharing flows within and among their agencies to determine the effectiveness of current processes and identify and resolve gaps in the WMD-T information sharing processes to facilitate the full incorporation of WMD-T information into the ISE.

4 Standardizing Procedures for Sensitive But Unclassified Information

"To promote and enhance the effective and efficient acquisition, access, retention, production, use, management, and sharing of Sensitive But Unclassified (SBU) information, including homeland security information, law enforcement information, and terrorism information, procedures and standards for designating, marking, and handling SBU information (collectively...must be standardized across the Federal Government."

— Guidelines and Requirements in Support of the ISE, Guideline 3

Providing an effective and efficient process for marking, handling, and sharing SBU information securely is an essential requirement for the ISE.[30] SAR information, for example, only rarely is classified. But it is critical that SARs be clearly marked and exchanged only over networks that provide adequate protection against loss or unauthorized disclosure. There are two separate but related ISE initiatives in this area:

- Establishing a streamlined framework that rationalizes the policies and processes for marking and handling SBU information; and
- Ensuring that systems that process, store, or share SBU information take adequate measures to prevent it's loss or unauthorized disclosure.

4.1 2007-08 Progress

4.1.1 Standardizing Procedures for Sensitive But Unclassified Information

SBU information is currently shared according to an ungoverned body of policies and practices that confuse both its producers and users. Across the Federal Government today more than 100 unique markings and over 130 different labeling or handling processes and procedures are used for SBU information. The result is an unmanageable collection of SBU sharing practices that impede the proper flow of information between Federal, SLT, and private sector partners. This is a national concern because the terrorist threat to the nation requires that many communities of interest, at different levels of government, share this vital but sensitive information.

[30] Although the President's approval of the new CUI framework means that, for the ISE, all SBU information is now CUI, in this Report we continue to use the terms interchangeably because of the deep historical roots of the term "SBU." Over time, however, the term CUI will replace SBU.

The new CUI framework:

- Creates a single policy for the government, reducing over 100 different SBU markings to three:
  - Standard Safeguarding and standard Dissemination;
  - Standard Safeguarding and specified Dissemination; and
  - Enhanced Safeguarding and Specified Dissemination.
- Describes the mandatory standards for the designating, marking, safeguarding, and disseminating of all controlled unclassified terrorism-related information originated by the Federal Government and shared within the ISE, regardless of the medium used for its display, storage, or transmittal;[31] and
- Strongly encourages its adoption by SLT and private sector entities.

Once fully implemented, this Framework will:

- End confusion about proper access, handling, and control of unclassified information that needs protection;
- Instill confidence that identical rules apply to everyone using the CUI markings; and
- Provide clear guidance to SLT partners now confused by SBU markings.

On May 9, 2008, the President issued a memorandum requiring agencies to implement the CUI framework. In addition, the President designated the National Archives and Records Administration (NARA) as the Executive Agent. NARA, in coordination with a CUI Council, will govern the new Framework and oversee its implementation.

An example of Confusion:
Ten different Federal agencies use the marking "LES" for Law Enforcement Sensitive information; however, the term is not uniformly defined across these ten agencies nor are there common rules governing access to "law enforcement sensitive" information. Consequently, each agency decides how to control and to whom to disseminate LES. An individual can have access to LES information in one agency but be denied access in another.

4.1.2 Protected SBU Transport

The PM-ISE, at the request of ISC members, established an interagency working group to better understand the continuing proliferation of unclassified ISE networks and develop recommendations for a more coherent approach. The working group analyzed and documented the current SBU environment in an effort to better understand and

[31] There are certain important infrastructure protection agreements between the Federal Government and the private sector that, because of additional safeguarding requirements are not fully accommodated under the proposed CUI framework. As a result, these Federal regulations with their associated markings, safeguarding requirements, and dissemination limitations will be "grandfathered" into the CUI framework.

define the process, policy, and technology issues with sharing SBU information. The group's recommendations prioritized the need for protected unclassified connectivity among all ISE participants and the need for an "information attribute" based identity management solution. In summary, the group concluded that:

- The ability to share SBU information across the ISE is less robust than it should be because of a variety of factors including limitations on protected interconnectivity between agencies, adequacy of and accessibility to agency-level shared space, proliferation of user accounts, and lack of enterprise-level access control and identity management services; and
- Agencies do not always use protected email services or networks to transport email containing SBU.

After reviewing Working Group findings, a majority of ISC members concluded that, although there are existing capabilities that can be exploited immediately to remedy some of these issues at minimal cost, there are no unaddressed Federal level mission imperatives that demand resolution of SBU connectivity and improvements to information sharing at the SBU level today.

4.2 Next Steps

4.2.1 Implementing the CUI Framework

The first step is to stand-up the CUI Executive Agent and the CUI Council. After initial stand-up is complete, the CUI Executive Agent, NARA, in coordination with the CUI Council, will manage and oversee the implementation of the CUI framework.

4.2.2 Protected Transport

It is imperative that Federal agencies protect the confidentiality, integrity, and availability of information stored, processed, and transmitted on SBU systems and ensure the authentication of access to such systems, as required. At the State and local level, challenges exist with managing multiple, competing, or duplicative information systems; redundant information from multiple systems; and limited ability to receive and share information with those who need it.[32] Planned activities include:

- Taking appropriate measures in support of U.S. policy, strategy, guidelines, and implementation actions to secure cyberspace, taking appropriate measures to reduce the risk to terrorism-related SBU systems and information stored on these systems and adequately deter, reduce, and limit the loss of information or the operational degradation of information systems critical to the ISE; and

[32] *Federal Efforts Are Helping to Address Some Challenges Faced by State and Local Fusion Centers* (GAO-08-636T), (April 17, 2006).

- Working with the ISC State and Local Subcommittee to determine those SBU network and service improvements that State and local partners view as important and the implementation priorities they deem appropriate. Based on insights gained, and leveraging the knowledge from the FY 2008 ISE SBU Network systems assessment, the activity will focus on the Law Enforcement and Homeland Security communities, leading to improved connectivity between agencies at all levels.

5 Sharing with Foreign Partners

"The ISE must support and facilitate appropriate terrorism information sharing between executive departments and agencies and foreign partners and allies."
— Guidelines and Requirements in Support of the ISE, Guideline 4

Recommendations in the Presidential Guideline 4 Report, as well as the NSIS, recognize that the "effective and substantial cooperation with our foreign partners requires sustained liaison efforts, timeliness, flexibility, and the mutually beneficial exchange of many forms of terrorism-related information."[33] The ISE fosters this cooperation by providing a community of interest in which ISC member agencies can collaborate on the bi-directional sharing of terrorism-related information with foreign partners, including the identification of best practices for negotiating foreign sharing agreements and development of standards for safeguarding and handling foreign government information.

5.1 2007-08 Progress

Formally established in March 2008, the interagency Foreign Partner Information Sharing Coordinating Committee, co-chaired by State and the PM-ISE, develops and provides tools and mechanisms that assist agencies in facilitating the sharing of terrorism information with foreign governments. 2007-08 progress in developing these tools includes:

- Issuance of the *Checklist of Issues for Negotiating Terrorism Information Sharing Agreements and Arrangements* to assist in the standardization of terrorism-related information sharing best practices by detailing internal U.S. Government considerations (including considerations around privacy information), considerations specific to the agreement or arrangement, and sources to consult during the agreement development and negotiation process.[34] As part of the spring 2008 measurement findings, two ISC member agencies reported having adopted the checklist in Department-wide processes.
- Stand-up of *a Repository of Foreign Sharing Agreements,* to allow ISE participants to identify and analyze existing, unclassified foreign agreements. Hosted on HSDN, and currently in the user acceptance test phase, the repository provides a user-friendly interface that allows agencies to access and review metadata and/or full text agreements.

[33] NSIS, op. cit., p. 26.
[34] *Checklist of Issues for Negotiating Terrorism Information Sharing Agreements* (ISE-G-101), PM-ISE (March 2008).

Furthermore, the NSIS rightly recognizes that the protection of privacy and civil liberties is essential to the successful sharing of information with our foreign partners. The U.S. is currently in negotiations with the European Union (EU) to develop a set of common principles for privacy and data protection for the information exchange between the U.S. and the EU. Although these principles are specific to the EU, the lessons learned, as well as the principles themselves, will also be applicable to other areas and regions that are partnering with the U.S. on the exchange of terrorism-related information.

5.2 Next Steps

Planned activities include the following:

- Continuing to identify government-wide best practices regarding internal procedures for expediting disclosure decisions and common standards or protocols for electronic handling of foreign government information in the ISE;
- Encouraging broad usage of the *Checklist of Issues for Negotiating Terrorism Information Sharing Agreements and Arrangements* to agencies responsible for the negotiation of foreign agreements and arrangements with foreign partners;
- Evaluating opportunities and, where appropriate, developing common foreign information sharing standards or protocols for the electronic handling of foreign government information within the ISE;
- Evaluating opportunities and, where appropriate, enhancing the *Repository of Foreign Sharing Agreements* to potentially include information on planned or ongoing negotiation activities;
- Determining how the U.S./EU privacy principles apply to the requirements of the Privacy Guidelines to ensure consistency in privacy standards across ISE member agencies and in negotiations with our foreign partners; and
- Ensuring that agency Privacy Act systems of records notices and routine use guidance provides for terrorism information sharing with foreign partners.

6 Protecting Privacy & Other Legal Rights

"[T]he Federal Government has a solemn obligation, and must continue fully, to protect the legal rights of all Americans in the effective performance of national security and homeland security functions."
— Guidelines and Requirements in Support of the ISE, Guideline 5

6.1 2007-08 Progress

Progress in protecting information privacy and civil liberties in the ISE is fundamental to creating a culture of information sharing. The ISE Privacy Guidelines create a uniform framework to help Federal agencies balance the dual imperatives of sharing information and protecting privacy by establishing uniform procedures for implementing required protections in specific legal and mission environments. The ISE PGC, with significant input from State and local members of the Global Justice Information Sharing Initiative (Global), has addressed issues relating to privacy guidance and facilitates, in consultation with the Privacy and Civil Liberties Oversight Board, the implementation of the Privacy Guidelines in ISE participant organizations. The PGC also periodically consults with civil liberties, privacy, and open government advocacy groups.

Over the course of the last year, the PGC has developed tools and resources to assist these agencies in identifying and resolving privacy and civil liberty related issues. Its efforts include the following accomplishments:

Fall baseline data revealed that 47% of agencies had established privacy policies that complied with the ISE privacy guidelines, a number that increased to 60% in the spring assessment. ISE agencies' adoption of the ISE Privacy and Civil Liberties Implementation Guide is expected to gradually (but significantly) increase the number of privacy-compliant agencies.

- Developed and released the *Privacy and Civil Liberties Implementation Guide* to help Federal agencies implement the *Privacy Guidelines;*[35]
- Developed the *Privacy Guidelines Implementation Manual* to serve as a single, comprehensive, resource to assist Federal Agencies in this process;

[35] The *ISE Privacy and Civil Liberties Implementation Guide* (September 2007) helps Federal agencies implement the ISE Privacy Guidelines. This Guide describes best practices and a methodology to ensure implementation of the protections and safeguards required by the *ISE Privacy Guidelines*. Available online at: http://www.ise.gov/pages/privacy-implementing.html.

Furthermore, the NSIS rightly recognizes that the protection of privacy and civil liberties is essential to the successful sharing of information with our foreign partners. The U.S. is currently in negotiations with the European Union (EU) to develop a set of common principles for privacy and data protection for the information exchange between the U.S. and the EU. Although these principles are specific to the EU, the lessons learned, as well as the principles themselves, will also be applicable to other areas and regions that are partnering with the U.S. on the exchange of terrorism-related information.

5.2 Next Steps

Planned activities include the following:

- Continuing to identify government-wide best practices regarding internal procedures for expediting disclosure decisions and common standards or protocols for electronic handling of foreign government information in the ISE;
- Encouraging broad usage of the *Checklist of Issues for Negotiating Terrorism Information Sharing Agreements and Arrangements* to agencies responsible for the negotiation of foreign agreements and arrangements with foreign partners;
- Evaluating opportunities and, where appropriate, developing common foreign information sharing standards or protocols for the electronic handling of foreign government information within the ISE;
- Evaluating opportunities and, where appropriate, enhancing the *Repository of Foreign Sharing Agreements* to potentially include information on planned or ongoing negotiation activities;
- Determining how the U.S./EU privacy principles apply to the requirements of the Privacy Guidelines to ensure consistency in privacy standards across ISE member agencies and in negotiations with our foreign partners; and
- Ensuring that agency Privacy Act systems of records notices and routine use guidance provides for terrorism information sharing with foreign partners.

7 Leveraging Ongoing Information Sharing Efforts

"The ISE shall build upon existing Federal Government policies, standards, procedures, programs, systems, and architectures...used for the sharing and integration of and access to terrorism information, and shall leverage those resources to the maximum extent practicable..."

— Guidelines and Requirements in Support of the ISE, Requirement 1

Although the PM-ISE, in consultation with the ISC, will continue to guide and oversee ISE implementation, as the ISE matures, agencies are ultimately responsible for implementation. Accordingly, they must take greater ownership of targeted outcomes, and be accountable for success as set forth in the agreed upon performance goals and measures. Leveraging ongoing information sharing efforts is an important element of the ISE. Other sections of this report include examples of initiatives that have served as building blocks for broader information sharing efforts. Highlights include:

- FBI-sponsored JTTFs combine Federal-State-Local units dedicated to combating terrorism in specific geographical areas.
- State and major urban area information fusion centers work closely with JTTFs and other Federal partners, and are dedicated to protecting our communities from all-crimes and all-hazards.
- Federal, SLT, and private sector governance structures such as the Federal CIO Council, the Global Justice Information Sharing Initiative, and the National Infrastructure Protection Plan sector partnership model, provide subject matter expertise and contribute directly to the development of ISE capabilities.
- The ISE EAF provides a common architectural structure for agencies to use to incorporate their information sharing capabilities into the ISE. ISC members, including DHS and DOJ, are adopting this architectural framework to enable their ISE participation. In addition, because it breaks new ground in several areas, others—notably the national health care communities—are now leveraging ISE EAF concepts to help develop Information Sharing Segment Architectures to interface not only with the ISE but also with other missions supported throughout their communities.
- The CTISS program incorporates information exchange standards developed by DOJ's and DHS's NIEM program office as part of new ISE-wide functional standards. The first of these addresses the high priority NSIS requirement for a unified process for gathering, documenting, processing, analyzing, and sharing SAR information. In late 2007, PM-ISE, NIEM, and the DoD and DNI UCORE program offices formed a multi-agency partnership for developing new converged

information exchange standards supporting the Law Enforcement, Homeland Security, Defense, and Intelligence communities.

- The DoD-DNI Cross-Domain Management Office, an interagency initiative that is identifying solutions for exchanging information among different security classification levels and domains and ensuring a core group of cross domain solutions is available for use by both the defense and intelligence communities.

In addition to the examples above, there are two primary institutional enablers that allow for effective leveraging of ongoing agency efforts—successful ISE governance and a well-structured investment process.

7.1 ISE Governance

The overall governance of the ISE is described in Chapter 4 of the ISE Implementation Plan. This structure has worked well and will continue to provide top-level direction in accordance with IRTPA and the NSIS. In addition, the PM-ISE and the ISC have established a number of subordinate bodies to guide specific aspects of ISE implementation. These include:

- *The Senior Level Interagency Advisory Group* (SLIAG) that monitors and oversees implementation of the Guideline 2 recommendations;
- *The CTISS Committee* that identifies and recommends common standards for issuance by the PM-ISE, evaluates impacts and potential incompatibility issues with other Federal Government standards programs, and monitors CTISS implementation; and
- *The ISE-SAR Steering Committee* with membership from Federal agencies and SLT organizations who play leading roles in the development and maturation of the nationwide ISE SAR process.

As a means of facilitating information sharing within their own agencies and across the environment, 93% of agencies reported having established their own information sharing governance bodies. This measure is a positive indicator of ISE members taking steps to ensure that information sharing is appropriately addressed within their agencies.

Although this section highlights the interagency governance efforts, individual agencies are also establishing governance processes and institutions to make information sharing an integral part of their internal policy and business process structure. The DNI, for example, established the IC Information Sharing Office of Facilitation and Resolution in November 2007 to improve information sharing throughout the Intelligence Community and to serve as the single point of entry for the resolution of information sharing issues. If a case cannot be resolved, either party to the case may request referral to the DNI for a final decision. Other existing Federal and SLT governance structures such as the Federal CIO Council and the Global Justice Information Sharing Initiative (Global) provide subject matter expertise and input in the development of ISE capabilities

7.2 ISE Investment Planning

7.2.1 The ISE Planning Cycle

Investment oversight and planning are important parts of managing the ISE. Coordinated, cross-ISE investment planning provides insight into ISC members' programs and budgets and will help ensure that ISC member agencies include ISE initiatives in their out-year planning and investment efforts. Over the past year, the PM-ISE has assessed the costs associated with ISE priorities, and more importantly, forged close strategic partnerships with OMB and the NCTC Directorate of Strategic Operational Planning, resulting in issuance of coordinated budget guidance for ISE agencies and establishment of a repeatable investment management process through the *ISE Planning Cycle*.[36]

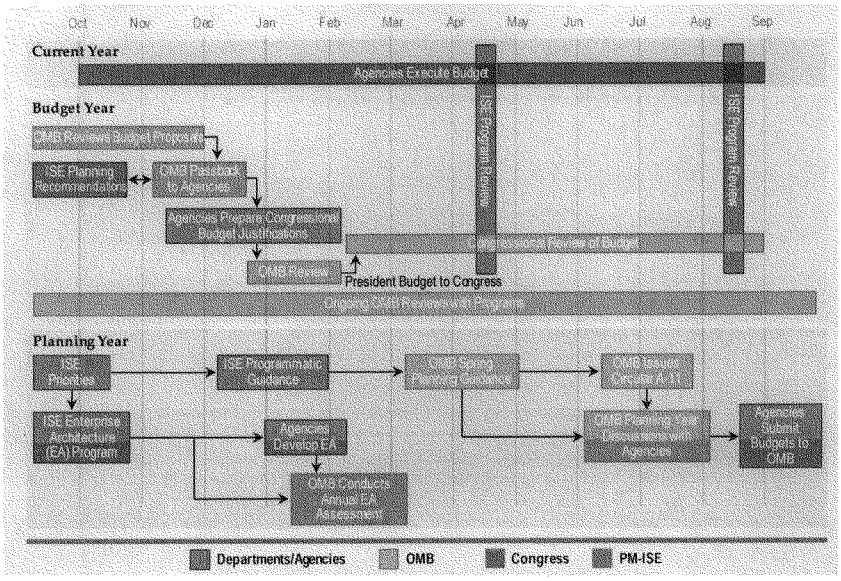


Figure 7-1. ISE Annual Planning Cycle

[36] The ISE Planning Cycle will further help "to ensure that procurement of and investment in systems and technology" are consistent with the direction of the ISE as required by IRTPA §1016(h)(2)(D).

The *Cycle* coordinates the ISE's strategic direction, resource planning, and program oversight. It is based on supporting OMB's existing processes and procedures and includes the steps involved in planning, programming, budgeting, and executing the resources necessary to institutionalize the ISE. Going forward, this Cycle (Figure 7-1) will help better coordinate the ISE's strategic direction, resource planning, and program oversight responsibilities.

7.2.2 Assessing Costs for ISE Priorities

Because ISE resources often account for only a small percentage of larger agency initiatives and are difficult to identify separately, the focus of ISE investment assessment efforts has been on costs associated with planning for and implementing specific ISE priorities. The PM-ISE developed such an assessment related to ISE-specific initiatives for FY 2007, providing an initial point of reference for future planning and budgeting. This effort created a foundation to better understand ISE expenditures and planned budgets addressing the intent of IRTPA to provide insight into the costs of developing and maintaining the ISE.[37]

Recognizing the challenge in separating out information sharing from larger mission operations costs, the effort focused on the costs associated with a limited subset of ISE priorities—those initiatives requiring a commitment of resources that would implement Congressional mandates and the President's priorities as outlined in the NSIS. For the FY 2009–13 planning cycle, these investment priorities are as follows:

- ISE-SAR Activities;
- State and Major Urban Area Fusion Centers;
- ITACG;
- SBU/CUI Framework Transition; and
- ISE Shared Spaces.

To better understand these investment priorities, the PM-ISE conducted a series of program reviews, requesting that ISE agencies provide cost data for FY 2007-09 associated with these priorities. The reviews were closely coordinated with OMB to ensure that the results could be incorporated into broader budget guidance. Based on the results, OMB issued direction to agencies on specific ISE priorities. Moving forward, the ISE will measure performance of each of these priorities as a portion of its performance management approach. These program reviews will continue next year to better align ISE investment and Performance management activities and facilitate the integration of ISE Investments and Performance Management initiatives into agency management structures through out-year planning and increased involvement of Performance Improvement Officers.

[37] IRTPA, as amended, op. cit., §1016 (h)(2)(C).

8 Promoting a Culture of Information Sharing

"Heads of executive departments and agencies must actively work to create a culture of information sharing within their respective departments or agencies by assigning personnel and dedicating resources to terrorism information sharing, by reducing disincentives to such sharing, and by holding their senior managers and officials accountable for improved and increased sharing of such information."
— Guidelines and Requirements in Support of the ISE, Requirement 2

Fostering an information sharing culture may be the most formidable challenge confronting the ISE. In the post-9/11 world, a predisposition to share the right information with those who need it is not merely an option but a fundamental principle firmly grounded in law and regulation. The goal is clear, but achieving it will take dedicated effort. The NSIS states "We will...change government culture to one in which information is regularly and responsibly shared and only withheld by exception." ISE cultural change initiatives aim to ensure that this principle is clearly understood and that managers are held accountable for driving change in their agencies.

8.1 2007-08 Progress

Accomplishments in 2007-08 include:

- Development of an ISE-wide computer based core awareness training course to be released to ISE participants this summer. The course will be distributed in one of three ways depending on agency preference:
  - As a program compatible with agencies' Learning Management systems;
  - As a program that can be installed directly on agencies' websites; or
  - On a compact disk that be installed at a user workstation.
- Following distribution of the course, Federal agencies will ensure that personnel who support the CT mission receive this core awareness training, tailoring it to their particular needs or supplementing it with agency-developed mission-specific training. Performance goals and measures to track progress will be incorporated in the 2008-09 Report.

In addition to the ISE Core Awareness Training, ISE participants are required to develop tailored training programs that achieve specific, related, learning objectives. One-third of the agencies surveyed in the fall indicated that they had established and completed some form of training to increase information sharing awareness. This number increased to 47% in the spring assessment.

- Many agencies—including DoD, DHS, and DNI—have issued new or first-time information sharing policies and strategies. The DNI's information sharing strategy, for example, is based on the premise of changing the IC from a "need to know" culture to one that embraces the principle of "responsibility to provide."
- DoD is assessing individual performance against information sharing practices and incorporating incentives into personnel processes and systems.
- Several organizations, including the ODNI and the Intelligence Division of the Department of Transportation, have incorporated information sharing as a factor in performance evaluations. Organizations are also beginning to include information sharing awards as part of departmental incentive programs. Overall participation improved from 40% last fall to 73% in this spring's performance assessment. As the DNI Information Sharing Strategy points out, "If ... personnel perceive that professional success is based in part on how well they share information, sharing *will improve* [emphasis added]."

Last fall, 27% of ISE agencies ISC member agencies reported initial steps to ensure accountability for information sharing via performance appraisals. The number grew to 47% this spring, with several agencies requesting assistance from OPM.

- DHS provides recognition, cash awards, time off, and other rewards when information sharing leads to the identification or apprehension of an individual posing a threat to national security.
- Many ISC members have established information sharing management boards and promulgated polices to promote sharing through techniques such as "write to release" and have modified practices that inhibit information sharing.

In the fall assessment, 53% of agencies were able to identify steps they took to remove information sharing disincentives in the areas of document dissemination (e.g., reduced use of originator controls), writing for release, and policies for sharing between internal departments. This number increased to 73% for the spring assessment.

8.2 Next Steps

Programs intended to create cultures of sharing will continue to evolve in the upcoming months to influence employee performance appraisals, awards and incentives programs, training, and initial implementation of the *ISE Privacy and Civil Liberties Implementation Manual.* Planned activities include the following:

- Enabling personnel who support the CT mission to receive the core ISE awareness training as the core training modules are developed. This training will be tailored to particular needs of personnel or be supplemented with agency-developed, mission-specific training;

- Expanding information sharing training to include courses responding directly to ISE priorities such as SAR. In addition, training guidelines for SLT entities will be developed by DOJ and DHS in coordination with other ISC members; and
- Partnering with OPM to assist agencies in adding information sharing elements to performance appraisals and incorporating information sharing incentives into personnel practice.

9 2009 ISE Performance Goals

IRTPA requires "objective system-wide performance goals for the following year."[38] In compliance with this requirement, the 2009 Performance Goals focus on:

1. Ensuring further development of initiatives related to the Presidential Guidelines and Requirements that are not yet sufficiently mature (e.g., Foreign Government Information Sharing; implementation of ISE Privacy Guidelines);
2. Further evolution and agency implementation of initiatives related to the Presidential Guidelines and Requirements that are based on actual operations with cross-cutting priority mission areas including SAR and AWN; and
3. Agency focused implementation activities.

The goals are designed to determine (1) the activities required to achieve anticipated 2008-2009 ISE outcomes and (2) the objectives and measures to track progress against these planned implementation efforts (Table 9-1).

Upcoming ISE performance management efforts linking 2009 Performance Goals to supporting objectives and measures will bring the ISE even closer to complying with the Presidential guidelines and requirements and the NSIS. This linkage will also provide the PM-ISE and the ISC with a means to better determine whether ISE initiatives are having their intended effect. ISC member agencies will use this assessment to identify areas where they can better build their capacity for information sharing. A line of sight from the 2009 Performance Goals to further maturation of specific ISE activities identified in the President's Guidelines and Requirements will provide the PM-ISE and the ISC with data to demonstrate the ISE's value to the next Administration, Congress, and beyond.

Table 9-1. 2009 ISE Performance Goals

2009 ISE Performance Goals
To further create a culture of sharing, agencies will: • Ensure all personnel charged with sharing terrorism information complete ISE awareness training. • Make information sharing a factor in awards and incentives programs. • Add information sharing elements to employee performance appraisals. • Complete Stage 1 of the *ISE Privacy and Civil Liberties Implementation Manual.*
To further reduce barriers to sharing, agencies will: • Implement ISE Shared Spaces. • Begin to adopt the Controlled Unclassified Information (CUI) Framework. • Work toward security reciprocity among Federal/State/local and private sector entities, to include people facilities and systems.

[38] IRTPA, as amended, §1016(h)(2)(B).

2009 ISE Performance Goals
To improve sharing practices with Federal, State, local, tribal and foreign partners, agencies will: • Make the ITACG fully-functional. • Increase fusion centers' access to terrorism-related information and ISE capabilities. • Make available to the appropriate personnel tools and mechanisms for the negotiation of terrorism-related agreements and arrangements. • Complete initial efforts to establish a national process for suspicious activity reporting.
To institutionalize sharing, agencies will: • Further integrate their IT management structures with ISE Enterprise Architecture principles. • Adopt ISE standards. • Further integrate ISE investment and performance management initiatives into department and agency management structures through out-year planning and increased involvement of Performance Improvement Officers.

Appendix A – Summary of the Alignment Between the NSIS and ISE Accomplishments

National Strategy for Information Sharing Core Principles and Understandings[39]	Alignment to ISE Accomplishments
Effective information sharing comes through **strong partnerships among Federal, State, local, and tribal authorities, private sector organizations, and our foreign partners and allies**.	• Established the ITACG and initiated development of an integrated network of fusion centers to enable the effective sharing of terrorism-related information between Federal and SLT partners. • Provided common tools and mechanisms that assist departments and agencies in facilitating the sharing of terrorism information with foreign governments.
Information acquired for one purpose, or under one set of authorities, might provide unique insights when combined, in accordance with applicable law, with seemingly unrelated information from other sources, and therefore we must **foster a culture of awareness in which people at all levels of government remain cognizant of the functions and needs of others and use knowledge and information from all sources to support counterterrorism efforts**.	• Completed an ISE-wide information sharing training course to be available to ISC member agencies this summer. • Replaced of the restrictive Cold War tenet of "need to know" by the principle of "responsibility to provide." • Efforts underway or in place to include information sharing as an important factor in personnel evaluation and awards and incentives programs. • Worked with fusion centers and local law enforcement departments to integrate a standard ISE-Suspicious Activity Reporting (SAR) business process into the day-to-day operational environments of their region.
Information sharing **must be woven into all aspects of counterterrorism activity**, including preventive and protective actions, actionable responses, criminal and counterterrorism investigative activities, event preparedness, and response to and recovery from catastrophic events.	• Established the ISE standards program and published the first ISE functional standard that institutionalizes an integrated ISE SAR process. • Leveraged the fundamental concepts of the *ISE Enterprise Architecture Framework* (EAF) and *ISE Profile and Architecture Implementation Strategy* (PAIS) by DOJ, DHS, and others for applications broader than the ISE. • Established the CTISS program and issued the *ISE SAR Functional Standard*. CTISS are business process-driven, performance-based "common standards" for preparing terrorism information for maximum distribution and access within the ISE. The SAR Functional Standard provides the data and information sharing foundation for operational information sharing of SAR in the ISE and supports demonstrations to include the SAR Evaluation Environments and an effort by the LAPD to redefine its SAR law enforcement processes. • Demonstrated the ISE EAF and CTISS in operational pilots. • Incorporated the ISE performance and investment strategy to provide the programmatic foundation for further institutionalizing the ISE.

[39] NSIS, op. cit., p. 2.

***National Strategy for Information Sharing* Core Principles and Understandings**[39]	**Alignment to ISE Accomplishments**
The procedures, processes, and systems that support information sharing must **draw upon and integrate existing technical capabilities and must respect established authorities and responsibilities**.	• Released the ISE EAF, a strategic guide for mapping ISE participants' enterprise architectures into the Government's FEA. The ISE-EAF provides a roadmap to enable long-term, institutionalized technology improvement and information systems planning, investing, and integration to support the sharing of terrorism-related information and identifies the network interfaces and standards needed to facilitate information sharing. • Ensuring that the CTISS Program incorporates information exchange standards developed for CTISS by DOJ's and DHS's NIEM program office into new ISE-wide functional standards.
State and major urban area fusion centers represent a valuable information sharing resource and **should be incorporated into the national information sharing framework**, which will require that fusion centers achieve a baseline level of capability to gather, process, share, and utilize information and operate in a manner that respects individuals' privacy rights and other legal rights protected by U.S. laws.	• Supporting improved collaboration at the State and local levels by leveraging fusion centers "as the primary focal points within the State and local environment for the receipt and sharing of terrorism-related information" and by establishing and sustaining a national integrated network of these centers

Appendix B – Acronyms and Abbreviations

AWN	Alerts, Warnings, and Notifications
ARJIS	Automated Regional Justice Information System
BJA	Bureau of Justice Assistance
C&A	Certification and Accreditation
CA	California
CI/KR	Critical Infrastructure/Key Resources
CICC	Criminal Intelligence Coordinating Council
CIIMS	Critical Infrastructure Inspection Management System
CIO	Chief Information Officer
CJIS	Criminal Justice Information Services
CP	Counterproliferation
CT	Counterterrorism
CTISS	Common Terrorism Information Sharing Standards
CUI	Controlled Unclassified Information
DHS	Department of Homeland Security
DNI	Director of National Intelligence
DoD	Department of Defense
DOJ	Department of Justice
EA	Enterprise Architecture
EAF	Enterprise Architecture Framework
EU	European Union
FBI	Federal Bureau of Investigation
FEA	Federal Enterprise Architecture
FIPS	Federal Information Processing Standard
FY	Fiscal Year
HIR	Homeland Intelligence Reports
HSDN	Homeland Security Data Network
HSIN	Homeland Security Information Network
IA	Information Assurance
IACP	International Association of Chiefs of Police
IC	Intelligence Community
ICE	Immigration and Customs Enforcement
ICEPIC	ICE Pattern Analysis and Information Collection System
IEPD	Information Exchange Package Description
IP	Implementation Plan
IRTPA	Intelligence Reform and Terrorism Prevention Act of 2004

ISC	Information Sharing Council
ISE	Information Sharing Environment
ISE EAF	Information Sharing Environment Enterprise Architecture Framework
IT	Information Technology
ITACG	Interagency Threat Assessment and Coordination Group
JTTF	Joint Terrorism Task Force
LAPD	Los Angeles Police Department
LE	Law Enforcement
LEO	Law Enforcement Online
LES	Law Enforcement Sensitive
LEISP	Law Enforcement Information Sharing Program
LEXS	LEISP Exchange Specification
LInX	Law Enforcement Information Exchange
MSP	Maryland State Police
NARA	National Archives and Records Administration
NCIS	Naval Criminal Investigative Service
NCTC	National Counterterrorism Center
N-DEx	National Data Exchange
NFCCG	National Fusion Center Coordination Group
NIEM	National Information Exchange Model
NIPP	National Infrastructure Protection Plan
NIST	National Institute of Standards and Technology
NSIS	National Strategy for Information Sharing
NSS	National Security Systems
ODNI	Office of the Director of National Intelligence
OMB	Office of Management and Budget
OPM	Office of Personnel Management
PAIS	Profile and Architecture Implementation Strategy
PDA	Personal Digital Assistant
PGC	Privacy Guidelines Committee
PM-ISE	Program Manager, Information Sharing Environment
R-DEx	Regional Data Exchange
RISS	Regional Information Sharing System
SAR	Suspicious Activity Reporting
SBU	Sensitive But Unclassified
SCI	Sensitive Compartmented Information
SIPRNET	Secret Internet Protocol Router Network
SLIAG	Senior Level Interagency Advisory Group
SLT	State, Local, and Tribal

TIDE	Terrorist Identities Datamart Environment
TN-ISPP	Tribal Nations Information Sharing Pilot Project
TSC	Terrorist Screening Center
TSDB	Terrorist Screening Database
TWPDES	Terrorist Watchlist Person Data Exchange Standard
TX	Texas
UCORE	Universal Core
U.S.	United States
WA	Washington
WMD	Weapons of Mass Destruction
WMD-T	Weapons of Mass Destruction – Terrorism-Related

Office of the Director of National Intelligence
Attention: Program Manager, Information Sharing Environment
Washington, D.C. 20511

(202) 331-2490

Visit us on the web at http://www.ise.gov

Statement for the Record of

CHARLES E. ALLEN

Under Secretary for Intelligence and Analysis
Chief Intelligence Officer
Department of Homeland Security

"Information Sharing at the Federal, State, and Local Levels."

U.S. Senate

Committee on Homeland Security and Governmental Affairs

July 23, 2008

Thank you, Chairman Lieberman, Ranking Member Collins, and Members of the Committee for the invitation to appear today. I know that information sharing has long been of special interest to this Congress and that your Committee played an integral role in directing the President to create an Information Sharing Environment for the sharing of terrorism information as part of the Intelligence Reform and Terrorism Prevention Act of 2004 (Intelligence Reform Act). So, I am pleased to have the opportunity to tell you about the real progress that the Department of Homeland Security, in cooperation with its Federal, State, local, tribal, territorial, and private sector partners, has made to ensure that the words "information sharing" are not a phrase repeated for political effect but rather reflect the inextricable relationship of information sharing to the primary DHS mission. I will explain how the Department is weaving information sharing into the fabric of its operations. Information sharing is an enabling function and core responsibility of every Departmental element, and as a result, will continue to improve regardless of transitions in leadership and organization.

The Department has heeded the calls from the President, as detailed in his *National Strategy for Information Sharing*, and the Congress to increase information sharing across the homeland security enterprise and create a culture based on the "responsibility to provide" information. But we recognize ensuring information gets to the right people does not happen automatically and cannot be left to chance. It requires dedicated efforts and constant attention as well as creating systems, processes, and environments that make sharing easier and more productive.

We have a statutorily mandated role in information sharing as prescribed by the Homeland Security Act of 2002. Creating the cultural and organizational infrastructure necessary to enhance the information sharing capabilities of the Department is a critical DHS mission to which we have devoted substantial resources. The efforts for improving information sharing throughout the Department are manifested in dozens of policies, mandates, and strategies issued since the Department was established and we are seeing results from these foundational efforts. One seminal policy regarding information sharing is the *DHS Policy for Internal Information Exchange and Sharing* that was signed by Secretary Chertoff on February 1, 2007. Referred to in the Department as the "One DHS" memorandum, its purpose is to promote a cohesive,

collaborative, and united Department-wide information sharing environment to reflect and complement the Department's similarly unified mission. The issuance of this memo provided essential direction to all of the Department's components and organizations to share information as part of a single enterprise. The Secretary expanded on his One DHS policy in May 2008 when he issued the *DHS Information Sharing Strategy*, which provides strategic direction and guidance for all DHS information sharing efforts, both internally and with external stakeholders, including Federal, State, local, tribal, private sector, and international partners.

While Ambassador McNamara has provided you with the State of the Information Sharing Environment writ large and the respective policies that have been put in place since the passage of the Intelligence Reform Act, I want to focus on how these concepts are being translated into action in this Department. I want to illuminate how the Department is building an information sharing governance structure to ensure the entire DHS enterprise can speak with one voice, and bring all of its information and knowledge to bear on preventing, protecting against, and responding effectively to threats against our homeland. I also want to describe the significant progress the Department has made in working with our Federal partners – most notably the DOJ/FBI, the DNI, and NCTC – to ensure that the Federal government is working in concert on these issues to maximize the benefit of our actions. Finally, I want to describe the myriad of ways DHS and our Federal partners work with our non-Federal partners to ensure that information is gathered and shared among all of us working to protect our country and all who live here.

DHS recognizes that a strong foundation is essential to long-term, sustainable improvements in information sharing. The governance structures we have built within DHS with my leadership as the Chief Intelligence Officer and the DHS Executive Agent for Information Sharing provide the essential foundation for the robust information sharing effort that our unified mission demands.

In April 2007, the Secretary established an Information Sharing Governance Board (ISGB) to serve as the executive level steering committee and decision-making body for all information sharing and collaboration activities within the Department. I currently serve as chair for the

ISGB. Other members currently include the principal leaders of the Offices of Policy and International Relations, Intelligence and Analysis (I&A), Operations Coordination, Infrastructure Protection, the Chief Information Officer, the General Counsel, and the designated Lead for the Law Enforcement Shared Mission Community, or LE-SMC (a rotating position presently encumbered by the Assistant Secretary for Immigration and Customs Enforcement). In addition, our Chief Privacy Officer and several other senior Departmental officials serve as *ex officio* members. The ISGB is the organization empowered to exercise the Secretary's ultimate decision-making responsibility on information-sharing matters.

Second, we have formed the DHS Information Sharing Coordinating Council (ISCC), an advisory, action-oriented body, fully representative of the Department's many organizational elements, that provides working-level deliberation and support to the ISGB. The ISCC is composed of Action Officers independently assigned by each of the Department's components and offices to represent their respective interests and perspectives. Among its many other responsibilities, this is the body that initially tackles the issues and tasks that are sent to the Department from the government-wide Information Sharing Environment.

Third, we are establishing Shared Mission Communities (SMCs) within DHS. The SMCs are cross-cutting information sharing efforts that bring together all of the relevant organizations within DHS that share common missions and objectives. They address the need to build integrated cultures, processes, and policies that facilitate information sharing across internal organizational boundaries.

The Law Enforcement Shared Mission Community (also known as the LE SMC) was the first shared mission community to be established and unites the full breadth of DHS law enforcement entities to enhance information sharing between components, other Federal agencies, and State, local and tribal law enforcement entities. This initiative has enabled the Department to create the Law Enforcement Information Sharing Service (LEIS Service) pilot, which unites DHS components and other Federal agencies to provide a single point of entry for Federal information sharing. Over time, this initiative will provide significant cost and resource savings (thereby

reducing operational costs) including to the Department and our State and local partners and deliver benefits while standardizing methods and policies. These benefits include providing improved law enforcement information sharing, which will result in increased officer safety and enhanced law enforcement operation effectiveness to deliver on the Department's mission to protect and prevent threats against the general public and the Nation as a whole.

The LEIS Service allows for the effective and appropriate sharing of DHS law enforcement data with State and local authorities through the deployment of information sharing technologies and operating policies. This technology complies with the President's *National Strategy for Information Sharing* and is aligned to the Information Sharing Environment (ISE) architecture framework. Additionally, the LEIS Service has collaborated with the Department of Justice (DOJ) to leverage their existing OneDOJ network in locations where it is cost effective and begin to build the backbone of a unified Federal infrastructure, thereby avoiding duplicative costs incurred by building independent infrastructures. Additionally the LE SMC has collaborated with the Departments of Defense and State to determine if additional economies of scale exist. This initiative will enable the eventual establishment of one standard for information sharing across federal law enforcement entities.

The LEIS Service has been developed using the ICE Pattern Analysis and Information Collection (ICEPIC) system to share excerpts from subject records and closed cases. Additionally, memorandums of agreement have been established to ensure consistent governance with State, local and tribal partners. The service has been launched this year in San Diego and Los Angeles with favorable initial results. The LEIS Service is also scheduled for deployment in Arizona and Texas by the end of this year. A long term deployment schedule, including the National Capitol Region and Chicago, is under development.

While the Department's unified governance structure, consisting of the ISGB and ISCC, is the essential foundation for fulfilling the Department's information sharing mission requirements, achieving the mission requires people and tools. We have devoted significant resources to providing both of these. There is no place where this is more evident than our efforts to ensure a

two-way flow of information between our State, local, tribal, territorial, and private sector partners and the Federal government. As the Implementing the Recommendations of the 9/11 Commission Act (9/11 Commission Act) and the President's *National Strategy for Information Sharing* make clear, fusion centers are an essential part of this information flow and framework. Working closely with the Department of Justice, DHS has critical responsibilities for leading the Federal effort to work with States and major urban areas to establish fusion centers across the country and design policies and programs to integrate them into a national network. Fusion centers form a critical bridge for sharing information vertically between the Federal government and our partners, as well as horizontally across the States. DHS has taken the lead to integrate the fusion centers into the Information Sharing Environment.

I am the Department's Executive Agent for support to the fusion centers. Within my Office of I&A, my team established the Department's State and Local Fusion Center Program Management Office (SLPMO) to build essential relationships with the fusion centers. By the time the 9/11 Commission Act passed late last year and called for the establishment of a fusion center program office within the Department, the SLPMO was already operational and had been since June 2006, when the Secretary signed The Department of Homeland Security Support Implementation Plan For State and Local Fusion Centers.

As a Department we support fusion centers by deploying, through the SLPMO, DHS intelligence officers to the centers, providing grant funding for their development and operation, connecting networks and systems, and strengthening the relevant communities of interest. To date we have 25 officers deployed and serving in fusion centers and we plan to have 10 more deployed by the end of this year. These men and women serve at the front line for information sharing. By using their varied experiences and skills as intelligence professionals, they are providing State, local, tribal, territorial, and even other Federal partners with the information they need to keep America safe. These same skills permit them to cull the best of what fusion centers are collecting and analyzing and ensure that it gets to the appropriate people in other States and in the Federal government – building the National Fusion Center Network.

To ensure that the National Fusion Center Network is staffed by analysts across the country who make the best use of their access to National-level intelligence, my Office is providing or coordinating intelligence training at the fusion centers. In a mobile training format we have delivered the one-week long Analysis and Critical Thinking Skills Workshop to over 40 analysts; another 20 are receiving this training this week as we speak. Our plan is to get this training to an additional 140 analysts over the next year. Through the Office of the DNI, we are taking advantage of its Open Source Academy's classes as well. The Academy has provided several sessions of the week-long Introduction to Analytic Tradecraft and the 2-day Tools and Techniques classes directly to several fusion centers. We are also working to make the Basic Intelligence Threat and Analysis Course (BITAC) and the DNI's Analysis 101 available to as many State, local, and tribal analysts as we possibly can.

In addition to ensuring that the right people are in place to analyze the information that is being provided, DHS is committed to providing fusion centers with the information sharing tools they need to participate in the Information Sharing Environment. To do so, we are providing network connectivity at the classified and unclassified level that enables fusion center personnel, both our own DHS officers as well as State and local analysts, access to Federal systems and data sources.

At the Secret level, we are deploying the Homeland Secure Data Network (HSDN). To date, HSDN has been deployed to 23 fusion centers and we are working to deploy it to 17 more by the end of this year. Our primary constraint in achieving this goal is ensuring that enough fusion centers have upgraded their facilities and infrastructure to the necessary security standards for deployment of classified systems. Among other capabilities, HSDN provides access to NCTC On-line – a classified portal that maintains the most current terrorism-related information at the Secret level. HSDN also provides the fusion centers with a window into the National Intelligence Community that they can use for their own information needs, as appropriate. Ultimately, every State and Local Fusion Center (SLFC) with HSDN access will have its own webpage to which relevant State, local, and tribal products can be posted and made available to other fusion centers and broader communities, including the National Intelligence Community.

On the unclassified level, the Homeland Security Information Network's "Intelligence" portal (HSIN-Intelligence) provides more than 8,000 people with access to finished FOUO intelligence products. To foster collaboration and share best practices and lessons learned within the fusion center network, DHS sponsors the Homeland Security State and Local Intelligence Community of Interest (HS SLIC), a virtual community of intelligence analysts. Its membership has grown significantly in the past year and now has members representing 43 States, the District of Columbia, and seven Federal departments. I have also established a HS SLIC Advisory Board, which includes State and local leaders of the HS SLIC to advise me and the rest of I&A leadership on issues relating to intelligence collaboration with our non-Federal partners. Through the HS SLIC, intelligence analysts across the country collaborate via weekly FOUO threat teleconferences, bi-weekly Secret-level secure video teleconferences, and in a virtual community of interest within a restricted portion of the HSIN-Intelligence platform, to share intelligence information in an appropriately secure and privacy sensitive environment. Members are thus able to post intelligence products so that there is effective vertical information sharing between the States and the Federal Intelligence Community and horizontally between the States. In addition, I have established an HS SLIC conference series which includes both an annual nationwide analytic conference conducted at the Secret level each September, and at least one annual theme-oriented conference per region, also at the Secret level. Finally, we are also planning to introduce on HSDN a secure, virtual collaboration workspace capability similar to that now available to the HS SLIC within HSIN-Intelligence. This connectivity will further enable us and our partners to collaborate more effectively and efficiently at the Secret level. Through all of these varied activities, DHS is making the HS SLIC a significant contributor to the National Strategy for Information Sharing.

In addition to the network connectivity we are providing to fusion centers, the Department has also developed the Constellation / Automated Critical Asset Management System (C/ACAMS), a tool that supports fusion centers and other information sharing partners in support of the Department's mission of protecting critical infrastructure. C/ACAMS provides State, local, and private sector partners with a set of resources to collect and manage information related to critical infrastructures and to inject infrastructure information into fusion center analysis. This

information, when combined with terrorism threat streams, provides fusion center analysts and private sector infrastructure owners and operators with a context to understand risk and to target protection resources against those assets or systems with the highest risk profiles. C/ACAMS is currently deployed to fusion centers across the country and is used by over 2,000 State and local infrastructure protection analysts. The data they have collected on over 38,000 unique infrastructure assets is vital to the national effort to enable prevention, protection, response, and recovery activities.

DHS is working to ensure that the information we share is what our partners need. To further this effort we undertook a pilot project with six fusion center partners to examine the day-to-day information needs of the centers. By working with the DHS officers embedded in the fusion center, intelligence personnel at DHS headquarters and, most importantly, our State and local partners, my Office was able to develop a precise set of priority information needs for fusion centers.

The leader of this pilot said in his report that there was a need for clearer paths for information flows and greater participation by the State and local personnel in the development of the information. As a result of these insights, we changed how information flowed within the Department and created a single point of service for supporting our State, local, and tribal partners. By identifying a single access point within the Department and bringing broad departmental support to the fusion centers through the DHS National Operations Center, DHS mitigates the confusion our State, local, and tribal partners faced of how best to interface with a department of our size and complexity. Moreover, we are now seeing joint analytic products serving all levels of government and the private sector being written by fusion centers in conjunction with DHS and FBI. So far, this year, nine finished intelligence products were co-authored by DHS, fusion centers, and other partners. In addition, more than 150 Homeland Intelligence Reports (DHS intelligence products designed to take information collected by DHS and share with the broader national Intelligence Community) have been written this year, using information DHS has obtained from its State, local, and tribal partners. We would not have obtained this information, except through this critical partnership. Collaboration such as this is

precisely what the Congress and the president envisioned in directing our Nation's intelligence and law enforcement communities to improve information sharing.

Although my Office leads the Department's fusion center efforts, we are reaching out across the DHS enterprise to bring all of the Department's resources to bear. As one example, the SLPMO has close relationships with FEMA's Technical Assistance Branch and works together to provide a broad range of support to the fusion centers. FEMA and the Department of Justice's Bureau of Justice Assistance have created the Intelligence Liaison Officers Program and the Terrorism Liaison Program which are designed to ensure that information contained within the fusion centers reaches the street level police officer and firefighter, and just as important, provides them with a clearly defined pathway for providing information back to the center and through it to the Federal level. Grant and technical experts from both Departments jointly administer these programs.

In addition to these specific DHS initiatives, the Department is providing leadership to important multi-agency organizations dedicated to improving information sharing with our non-Federal partners.

An important piece of multi-organizational effort is the National Fusion Center Coordination Group (NFCCG) that was established as a working group under the Information Sharing Council, to assist the implementation of the recommendations approved by the President, and later incorporated into the *National Strategy for Information Sharing*, to establish a national integrated network of fusion centers. The director of my State and Local Fusion Center Program Management Office serves as co-chair of this important group with the Deputy Director of Intelligence at the FBI. The Group brings together key Federal partners from the FBI, DOJ, DHS, DNI, PM-ISE, as well as State and local organizational leaders to build the framework needed for effective information sharing.

The NFCCG has been successful in fostering the development of fusion centers and bringing them into a cohesive partnership at the State and local level as well as with their Federal partners.

One notable achievement of this Group is its coordination and sponsorship of a series of national and regional fusion center conferences. The two national conferences to date are widely considered by fusion center managers and personnel to have been highly productive and successful. Nearly 600 delegates attended in 2007 and we reached capacity this year at almost 900 attendees, with several hundred interested participants turned away. This has become the seminal information sharing conference for State, local, and tribal governments, fusion centers, and their Federal partners.

On the content side of this effort, the Interagency Threat Assessment and Coordination Group (ITACG) was established at the direction of the President and the 9/11 Commission Act to facilitate increased sharing of terrorism-related information between the National Intelligence Community and our State, local, tribal, territorial, and private sector partners. Too often in the past our non-Federal partners were confused by seemingly inconsistent information coming from various parts of the Federal government or complained that they lacked threat warning and assessment information. By pulling together in one place State, local, tribal, territorial, and Federal homeland security, law enforcement, and intelligence officers at the National Counterterrorism Center, there is now a focal point to guide the development and dissemination of Federal terrorism-related intelligence products through DHS and the FBI to our State, local, tribal territorial, and private sector partners.

Under law, the ITACG consists of two elements: the ITACG Detail and the Advisory Council. The Detail is the group of individuals who sit at the NCTC and conduct the day to day work of the ITACG. The Council is tasked with setting policy and developing processes for the integration, analysis, and dissemination of Federally coordinated information, as well as for providing oversight of the ITACG Detail and its work.

The Detail achieved Initial Operating Capability just six months ago on January 30, 2008. While fully integrated into the work and leadership at NCTC, the Detail is led by one of my senior intelligence officers who serves as the ITACG Director. The Deputy Director is a senior analyst

from the FBI. The FBI and my Office have each provided an additional senior analyst to help with the operation of the Detail Currently there are four law enforcement officers from State and local police departments, a tribal representative who works at NCTC, and two NCTC contractors with extensive experience in the intelligence community and State and local law enforcement. These non-Federal participants are assigned to assist the Detail and provide critical insight into the needs and perspectives of our State, local tribal and private sector partners. We are working hard to expand the number of non-Federal participants to ten in order to include a broad range of expertise, including fire and health departments, homeland security advisers, and other organizations as needed. Even as we seek to expand the membership of the IATCG, our primary focus remains on strengthening the ITACG by ensuring effective State and local law enforcement representation.

The members of the Detail have essential systems connectivity in NCTC, participate in key briefings, and are engaged in the NCTC production processes and activities so they have the broad perspective of the Intelligence Community. They can then act as an advocate for our State, local tribal and private sector partners by informing and shaping National Intelligence Community products to better meet the specific needs of the State, local tribal and private sector entities. They support the production of three types of reports: 1. alerts, warnings, notifications, and updates of time-sensitive information related to terrorism threats to locations within the United States; 2. situational awareness reports regarding significant events or activities occurring at the international, National, State, local, or tribal levels; and 3. strategic and foundational assessments of terrorist threats to the United States. In the event of conflicting reporting or, as the need arises, the ITACG facilitates Federal coordination to ensure that reporting on threat information is clear and actionable to the greatest extent possible.

The ITACG Detail has reviewed tens of thousands of finished intelligence products. As part of the review, the ITACG identifies products that meet State, local, and tribal needs, and ensures that they were disseminated appropriately to State, local, and tribal officials. The group has also has reviewed thousands of separate reports on worldwide threats to U.S. interests, identifying those that were possible threats to the Homeland. For a small number of these, the ITACG

Detail revealed that the reports were of questionable credibility, some of which required better characterization of the threat or source. As a direct result of the ITACG's efforts, DHS and FBI refined their characterization of the threat and released joint reports on two cases that required further threat detail.

We have also established the ITACG Advisory Council that I chair on behalf of the Secretary. The Council, at least 50 percent of whose members must represent State, local, and tribal organizations, has become a robust organization. Although the 9/11 Commission Act requires that it meet a minimum of four times a year, its work is too important and too pressing to meet so infrequently. Instead, we meet in person every other month. Four such meetings have been held to date. In the months when we do not meet in person, we hold a teleconference. This way critical issues and tasks do not linger before being tackled and resolved. These meetings address a number of priority challenges that we expect this new organization to face – especially recruitment of outstanding State, local, and tribal personnel to serve on the Detail, establishing an attractive Fellowship Program for the selected detailees, and developing formal mechanisms to ensure that information is getting to the right customers and creating a feedback process for State, local, tribal and private sector customers. Although progress on these issues has been slower than I wanted, we are starting to make major breakthroughs that will move the ITACG forward and ensure that it excels at its mission. I am proud of the team we have assembled – both for the Detail and the Advisory Council – and appreciate their continuing contributions to this critical work.

DHS also is working with its Federal partners on a number of less visible but still very important efforts to improve information sharing. I want to highlight two notable examples of initiatives that are enhancing our capabilities: National Information Exchange Model (NIEM) and suspicious activity reporting (SAR).

In the last twelve months, DHS has dramatically increased its adoption of the NIEM. NIEM is a data standards management initiative co-sponsored by the Departments of Homeland Security and Justice with extensive participation by State and local stakeholders. The implementation of

the NIEM standard in an information technology (IT) system enables data to be translated into a common language and shared more easily with other IT systems. This effort is essential because without data standards, system-to-system data exchanges are often difficult, both within agencies and with external partners. Data standards like NIEM not only enhance our ability to connect the dots that exist in numerous IT systems, they also enhance our ability to categorize data and ensure appropriate user access and usage in accord with privacy and civil liberties rules.

Across the Department, components such as DNDO, CBP, FEMA, ICE, NPPD, S&T, TSA, USCIS and US-VISIT are realizing these opportunities through NIEM adoption within major IT investment programs. These opportunities, such as those being built at ICE in support of law enforcement information sharing, will improve the way information is shared with State, local and tribal partners. Additional opportunities will include improving screening against the terrorist watchlist, defining exchanges in support of radiological nuclear detection systems, and the creation of person-centric query capabilities that will enable agencies, such as USCIS, to gather information from DHS and Department of State systems to build a comprehensive picture of an individual to support the immigration benefit determination process.

NIEM adoption is also happening at the State and local level. As part of the Homeland Security Grant Program, DHS requires all grantees to use the latest NIEM specifications and guidelines regarding the use of Extensible Markup Language (XML) for all HSGP awards. DOJ has the same requirement for several of its grant programs. Far from resisting this imperative, our State and local partners are embracing the adoption of NIEM because it enables information sharing with Federal government systems and across State and local jurisdictions.

In early July, the HSIN-Intelligence platform began establishing, in coordination with the Department of Justice and the Program Manager for the Information Sharing Environment, federated access capabilities across a number of other information sharing platforms such as Law Enforcement Online (LEO) and the Regional Information Sharing System Network (RISSNet). For the first time, DHS has allowed appropriate Department of Justice users of these other platforms direct access to DHS finished intelligence products residing on HSIN-Intelligence

without requiring separate password or login requirements. By making access to multiple systems easier, we hope to reduce the gaps in knowledge that might occur from accessing only one system.

In addition, DHS and its Federal partners have made significant progress in their efforts to coordinate an effective, unified strategy for the handling of suspicious activity reporting (SARs). Using SARs has been identified as a capability to begin to see seemingly disparate activities that, when overlapped, show a pattern and possible threats. By designing a system that incorporates procedures and actions that begin at the State, local, and tribal levels, and are supported at the Federal level, DHS' ability to review, analyze, and further disseminate important information that is collected by non-Federal partners is significantly enhanced.

Across the country, DHS has worked closely with local jurisdictions, including Los Angeles, Miami, Boston and Chicago, to understand their approach to SARs and how to best promote cross-integration. By identifying "best practices" at the State, local, and tribal levels, the Federal partners are able to build a collaborative SAR approach.

All of the Federal activities in SARs continue to carefully maintain the balance between the protection of its citizens and the protection of its citizen's privacy and civil liberties. There are standing working groups and committees involving the General Counsel, Privacy, and Civil Rights / Civil Liberties Offices, of the Federal Departments involved in suspicious activity reporting.

We must remember, however, that increased information sharing comes with responsibilities. We are ever mindful that all of these efforts discussed today must be conducted with civil liberties and privacy rights at the table. To that end, our Privacy and Civil Rights Offices have delivered training to all of our deployed officers and are working with Bureau of Justice Assistance and PM-ISE to develop training for State, local, and tribal representatives in the fusion centers. We are also developing Privacy Impact Assessments for these efforts.

While these particular accomplishments of these inter-agency organizations such as the NFCCG and the ITACG and these other examples of multi-agency collaboration are important in their own right, they are particularly notable because of the close relationships among DHS, FBI, DOJ, the DNI, the PM-ISE, and the many State and local leaders that make them possible. It is these relationships in conjunction with the framework that is being created that makes information sharing a routine occurrence rather than a special event.

Conclusion

I have touched on a broad range of information sharing activities involving the Department and its valued partners because I wanted to give the Committee a sense of the extraordinary efforts DHS is making to foster information sharing at all levels of government. Information sharing is not, and cannot, be an afterthought or a sideline activity. It is not merely incidental to, but rather essential to and, indeed, a vital piece of our mission. We remain committed to implementing the information sharing mandates of the Intelligence Reform and Terrorism Act of 2004, the Homeland Security Act of 2002, and the recently passed 9/11 Commission Act, while continuing to protect civil liberties and privacy.

Thank you and I look forward to your questions.

TESTIMONY

SENATE COMMITTEE ON HOMELAND SECURITY & GOVERNMENTAL AFFAIRS
Wednesday, July 23, 2008

Prepared Statement of James M. Thomas, Commissioner,
Department of Emergency Management and Homeland Security,
State of Connecticut

OPENING COMMENTS

Senator Lieberman, Senator Collins and members of the Committee, good morning and thank you for inviting me here today. My name is James M. Thomas and I am the Commissioner of the Connecticut Department of Emergency Management and Homeland Security. I am here to talk to you about the Intelligence Reform Act of 2004.

I do want to tell you that in my 39 years of law enforcement experience I have never seen such a strong willingness to share information among the local, regional, state and federal partners. It is clear that the Department of Homeland Security (DHS) has been working very closely with state entities in developing strong collaborative teams in this regard. I have participated in and have seen the benefit of this collaborative approach not only in Connecticut but also throughout the country. DHS has set standards for information sharing. Most states and large urban areas have been moving towards the adoption and implementation of important standards. In the field these standards specify what are known as "Fusion Centers" or "Intelligence Centers." DHS has been a leader in providing training, expertise and assistance to all of the 50 states and U.S. Territories regarding intelligence centers in an effort to further develop this critical mission, which when successful will help prevent terrorist attacks from abroad or home grown.

The key to effective terrorism prevention activities is "good" timely intelligence. The motto of intelligence sharing should be... "Gather" – "Evaluate" - "Analyze" and then "Share" information. I can tell you that in our part of the country information sharing has never been better. For example... This past week and every week, intelligence information is shared with 169 municipalities in our state and it includes information from local law enforcement, State Police, Department of Corrections and federal agencies such as the Federal Bureau of Investigation (FBI), Alcohol, Tobacco and Firearms (ATF), Drug Enforcement Agency (DEA), the Transportation Security Administration (TSA) , the U.S. Coast Guard and the Department of Homeland Security (DHS). The Connecticut Intelligence Center (CTIC) weekly bulletin also has information from the states of New York, Rhode Island, Massachusetts and New Hampshire.

In addition, to the weekly bulletin, we can issue daily and hourly bulletins, if needed and appropriate. The officers in the field can and do receive this material on their mobile data terminals within their police vehicles. Clearly this is critical as the end user the officer, trooper or other law enforcement professional needs to have timely, vetted credible information in order to do their job effectively. There is too much at risk if we do not share the information with them, as they are the men and women who are on the front lines and serve as the best means of preventing or stopping a terrorist incident from happening.

Coming from a local law enforcement agency and serving in that capacity as a Chief of Police in two communities, I truly believe that the most effective and efficient means of gathering information and ultimately using that information MUST be done at the local level. In Connecticut we have accomplished this by establishing five (5) Regional Intelligence Officers (RILOS) whose job is to gather and exchange information between the local level and CTIC.

This past week and every week as I speak with local law enforcement, they have indicated that the information sharing they receive has never been as good as it is at this time. This is truly the efforts of everyone, especially with the efforts of Charlie Allen and his team at DHS. Mr. Allen, as you know, brings many years of credible intelligence sharing experience to the table and through his efforts and the efforts of other federal agencies, they have been assisting the local and state agencies in meeting the standards of information sharing.

In addition, we also believe that we need to fully engage the "Private Sector" and again through the efforts of DHS we have been able to develop a weekly bulletin for the private sector that is hosted on the secure Homeland Security Information Network (HSIN) that provides them with very timely open-source information at the local, state, regional, national and international levels. We believe that this sharing of information with the private sector will again pay dividends as we have a very active collaborative relationship with the private sector.

Clearly times have changed. The threat for terrorism related activities is real and a constant concern. So the way we do business needed to change. This change is now taking place… We believe and hope that your committee will continue to support and fund the fusion/intelligence centers that have been developed and will support our goal of having well trained intelligence analysts from the federal, state and local agencies working side-by-side analyzing the information and intelligence they receive and most importantly… disseminating it back out to the street where it needs to be shared to have the most profound impact.

This past March the Department of Homeland Security in partnership with the Department of Justice sponsored a National Fusion Center Conference. All 50 states and several of the U.S. Territories attended the conference and it was clear that we need to continue in the direction of sharing credible information in a timely manner. Together we can and will make a difference. We do need to work together like we've never done before in order to make the entire United States and world a safer place. We need to work together to get the information to the most effective agents of change, our local first responders, whom I call our "First Preventers."

Again, thank you for giving me an opportunity to share my thoughts with you today. I would be happy to answer any questions you might have.

Testimony
Jeffrey H. Smith[1]
Senate Committee on Homeland Security & Governmental Affairs
July 23, 2008

Mr. Chairman, Senator Collins, it is a privilege for me to appear before this Committee today to discuss an issue of significant importance to our national security: ensuring that the right people have the right information at the right time.

The terrorist attacks of September 11th and the dynamic threat of global terrorism prompted an introspective review of the failures of American intelligence and, especially, how information is shared and how government agencies collaborate. I hope my comments today will give this Committee a better sense of how far the government has come toward a trusted information sharing environment and how far it still has to go.

Under the leadership of Zoe Baird and former Netscape CEO, Jim Barksdale, the Markle Foundation convened a bipartisan Task Force, of which I am a member, to examine national security in the information age.[2] This diverse group has consulted with government officials, private industry, experts on technology and civil liberties, and foreign partners in order to find solutions for this critical information sharing problem. Through a series of reports, the Markle

---

[1] Senior Partner, Arnold & Porter LLP; former General Counsel, Central Intelligence Agency; and former General Counsel, Senate Armed Services Committee.

I am grateful for the assistance of Nicholas Townsend, an associate at Arnold & Porter, and Manav Bhatnagar and Daniel Bernstein, summer associates from Yale Law School and Stanford Law School.

[2] I am appearing today at the request of the Committee on my own behalf. Although I have consulted with members of the Markle Task Force in the preparation of my testimony, I am here in a personal capacity and not as an official representative. I do not speak for the Markle Task Force. A listing of all the Task Force members is attached to my testimony.

Task Force has advocated for the creation of a trusted information sharing environment that achieves the twin goals of national security and civil liberties.[3] The Task Force has worked closely with government officials, and I am pleased to report that the government has taken many of our recommendations to heart. The country has adopted important reforms through legislation, executive orders, and national strategies to facilitate the flow of information among the federal government, state and local agencies, the private sector, and foreign partners. This Committee deserves special recognition for the role it has played in these reforms.

As the GAO found in the report it released today on the information sharing environment, although the Congress, President, and intelligence community have made progress, much still needs to be done. Significant cultural, institutional, and technological obstacles remain. Our nation cannot allow recent reforms or the absence of a new attack on our homeland to lull us into complacency. There is reason to be concerned that the initial focus and momentum have dissipated, while confidence in the process and deliverables have decreased. To meet modern national security challenges, we must renew our commitment to greater information sharing consistent with respect for privacy.

As the Task Force articulated in its three reports, an effective information sharing environment must be built on trust. The agencies of government must trust each other with sensitive information, and the American people must trust their government to protect their civil

[3] *See* MARKLE FOUND. TASK FORCE, MOBILIZING INFORMATION TO PREVENT TERRORISM (2006); CREATING A TRUSTED INFORMATION NETWORK FOR HOMELAND SECURITY (2003); and PROTECTING AMERICA'S FREEDOM IN THE INFORMATION AGE (2002), *available at* http://www.markle.org/markle_programs/policy_for_a_networked_society/national_security/projects/taskforce_national_security.php.

liberties and privacy. Realization of this trusted environment urgently requires: (1) sustained leadership and strong oversight from all branches of government; (2) clear policies, processes, and guidelines that facilitate collaboration and sharing of information while protecting civil liberties; and (3) technologies that facilitate sharing while protecting security and privacy.

Information sharing must not be a partisan issue; it goes to the core of good governance. To this end, the Markle Task Force continues to assess the government's progress and is currently preparing a report card that will make constructive recommendations to give to the next president and to Congress that will help the nation move its information sharing system forward.

I. Leadership on Intelligence Reform and Information Sharing

Creating a trusted information sharing environment requires leadership throughout the government.

Congressional leadership is needed to pro-actively exercise oversight responsibilities and provide adequate funding for the implementation of information sharing provisions. In response to various study group reports, Congress has passed landmark legislation such as the USA PATRIOT Act, the Intelligence Reform and Terrorism Prevention Act of 2004, and the Implementing Recommendations of the 9/11 Commission Act of 2007. These acts have removed obstacles to information sharing and established procedures for implementing further reforms. Importantly, Congress has also held regular oversight hearings, such as this one, to keep the government on the right track. To make additional progress, Congress should

streamline the jurisdiction of its oversight and appropriations committees, and expedite the confirmation of political appointments to the intelligence community and its oversight bodies.

Presidential leadership is also necessary to steer implementation across agencies, facilitate the kind of cultural transformation that is required, and encourage public confidence in the government's information sharing policies. Through executive orders and memoranda, the President has made the creation of a trusted information sharing environment a priority within the executive branch. The White House has recently issued a comprehensive information sharing strategy, standardized the classification system, and streamlined the security clearance process. The President also established the National Counter Terrorism Center (NCTC) in 2004, which serves as a centralized clearinghouse for all intelligence related to terrorism and counterterrorism. While these are steps in the right direction, the President should renew his commitment to trusted information sharing and exercise greater leadership in implementing specific recommendations from recent intelligence reform legislation so that this momentum is not lost.

Earlier this year, the Director of National Intelligence released his first-ever Community Information Sharing Strategy, and Ambassador McNamara, the Program Manager for the Information Sharing Environment, has now presented his second annual report to Congress. These executive branch efforts have initiated a paradigm shift from a "need to know" to a "need to share" culture. I greatly appreciate Ambassador McNamara's efforts and the leadership of Charlie Allen in the effort. I also welcome the GAO's recent report to Congress on the information sharing environment and recognize the importance of defining the ISE's scope and

measuring its performance. However, the Administration must ensure that transforming government in order to improve information sharing and collaboration is an urgent priority that does not wane or fall victim to turf battles and ambiguity about responsibility and authority.

Finally, leadership is needed at the state and local level to improve coordination, standardize information sharing procedures, and evaluate progress. There has been some progress on this front, as many state and urban areas have established "fusion centers" to coordinate information sharing and turn intelligence into actionable knowledge. However, it is unclear whether the fusion center model is the best approach; certainly, further work needs to be done to ensure information sharing among all levels of government and with the private sector.

II. Implementation Status of the Markle Policy Recommendations on Intelligence Reform and Information Sharing

Mr. Chairman, while there is now broad agreement on the need for greater information sharing, I believe that many of the relevant government actors have not yet internalized this priority.

I would like to turn to some of the most important policy recommendations of the Markle Task Force and discuss both the progress and shortcomings of the government in the pursuit of these goals.

First, a core recommendation of the Markle Task Force is the adoption of an *authorized use* standard. Under such a standard, agencies or employees could obtain mission-based or threat-based permission to access or share information, as opposed to the current system which relies on place-of-collection rules, U.S Persons status, and originator control (ORCON) limitations. Congress took a step in the right direction by asking the President to consider adoption of an "authorized use" standard in the Implementing Recommendations of the 9/11 Commission Act. However, one year later, the ISE Program Manager issued a "Feasibility Report" which argued against adopting such a standard because of perceived conflicts with existing privacy protections, as well as overlap with existing ISE privacy guidelines. I believe that the adoption of an authorized use standard is still a desirable and necessary goal. Although weight should certainly be given to the Program Manager's concerns, I am confident that an authorized use standard that is consistent with and respectful of security and privacy interests can be developed.

Second, the Markle Task Force has also called for the creation of a government-wide *dispute resolution mechanism* to replace the current cumbersome ad-hoc process. The 2007 Implementing Recommendations of the 9/11 Commission Act established the parameters, and affirmed the need, for a government-wide mechanism. Congress has also provided the Program Manager with the necessary authority, ability to hire, and funding to implement such a program. Such a system should be developed, as disputes between agencies during information sharing are inevitable, and should not be allowed to interrupt the functioning of the intelligence community.

Third, the Markle Task Force has emphasized the importance of protecting the *privacy and civil liberties* of our citizens through detailed guidelines. To earn the trust of government employees and the public, greater protections for privacy and civil liberties must accompany greater information sharing. The ISE has issued guidelines that require that information sharing complies with the Constitution and applicable laws, occurs only for a proper purpose, identifies protected information, is accurate and secure, and remains subject to audit. Accordingly, each agency must now develop a written privacy protection policy consistent with these guidelines. In the past year, the ISE has released helpful implementation instructions for the agencies. The next step is for the ISE Program Manager and the DNI to work with agencies to develop the kind of detailed and specific guidelines that are needed to support trusted information sharing. New policies may be needed that go beyond the Privacy Act and existing laws to address situations specific to information sharing. Even if the government can legally do something, prudence may require forbearance. For example, as the NCTC's Terrorist Watch List grows ever longer, more Americans' privacy and freedom of travel may be put at risk. It is therefore essential to have robust procedural controls in place.

To provide institutional oversight, the privacy guidelines also created a governance structure comprised of the ISE Privacy Officials from each relevant agency, the ISE Privacy Guidelines Committee, and the Privacy and Civil Liberties Oversight Board.
However, the Privacy and Civil Liberties Oversight Board that Congress created to review the effects of information sharing and to advise the president is currently inactive. Following the Board's first report in 2007, one of its members resigned because he believed that the Board interpreted its responsibilities too narrowly and lacked sufficient independence from the White

House. In response, Congress wisely reconstituted the Board as an independent agency within the executive branch. By statute, this new Board should have been up and running by January 30, 2008. It is regrettable that a full slate of new Board members has not yet been nominated or confirmed. Congress and the President should breathe new life into this important institution.

Fourth, the Administration and Congress have made significant progress on the Markle Task Force's recommendation to improve information sharing through *greater training and development of human capital*. The Information Sharing Environment Implementation Plan calls for departments and agencies to develop tailored training programs, a baseline training module, and incentives to encourage the adoption of an information sharing culture by holding personnel accountable. Similarly, the implementing recommendations of the 9/11 Commission Act of 2007 require the development of a curriculum and of training for employees of federal intelligence agencies, as well as state, local, and tribal officials with regard to information sharing processes. The third Markle Report also calls for the establishment of an entry-level evaluation administered to all employees of the intelligence community in order to promote information sharing skills, familiarity with technology, and a culture of trusted information sharing. This recommendation, however, has not yet been implemented.

Fifth, the Markle Task Force's recommendation for *improving the decision making* of officials by providing them with more diverse intelligence has seen progress. The intelligence community has acknowledged the shortcomings of existing analysis and placed a greater emphasis on considering divergent perspectives. For example, agencies have adopted "alternative analysis cells" to ensure more rigorous intelligence estimates. Some agencies have

also internalized the practice of including confidence assessments within reports to better assess the reliability of evidence. Further, the DNI created an Open Source Center to encourage the use of non-classified information. As a result, the President's briefing now relies on a more diverse intelligence base. To better inform decision-making, efforts should continue to create a unified open-source system.

Sixth, information sharing reforms have reflected the Markle Task Force's emphasis on *vertical integration of state, local, and private actors*. The Interagency Threat Assessment and Coordination Group (ITACG) has begun to support the NCTC by sharing "federally coordinated" information with other levels of government, and the Homeland Security Information Sharing Fellows Program now brings non-federal government analysts into the department. As noted earlier, state and urban areas around the country have also established "Fusion Centers." However, the legal and financial foundation for these efforts remains shaky. Unfortunately, state, local, and private actors are not fully integrated into the ISE. For instance, they do not currently sit on the Information Sharing Council as full members.

III. Adoption Status of Technology to Support Information Sharing

Finally, we must continue to develop and deploy technologies that support policies and processes to connect people and information. Congress reaffirmed the importance of the Markle Task Force's recommendations regarding immutable audit logs and anonymized information use technology in the Implementing Recommendations of the 9/11 Commission Act of 2007. These

technologies are designed to improve data sharing, enhance security, and facilitate privacy and accountability.

The Program Manager's "Feasibility Report" concluded that implementation of anonymization technology was not feasible because of shortcomings in existing technology, difficulty with integration into existing systems and processes, and complications related to re-identification. It is vital that resources be directed into overcoming the obstacles to a more technologically robust information sharing system that incorporates anonymization and audit technology. These technologies are essential to connect people who fight terrorism and to do so in ways that enhance trust in information sharing.

***

In conclusion, Mr. Chairman, it has been a great honor for me to appear before this Committee today. As you can see, the country has made significant progress toward the creation of a trusted information sharing environment that achieves the twin goals of ensuring national security and protecting civil liberties. Yet more needs to be done.

The Markle Task Force will continue to engage with the government on the critical national security issue of information sharing. In the coming months, the Markle Task Force will reach out to both presidential campaigns with specific recommendations for what steps need to be taken to ensure a trusted information sharing environment. The Markle Task Force will also continue to work with Congress as it develops further information sharing legislation. As I

described earlier, we need to implement additional policies that make information sharing a reality and we need to capitalize on the best technology available. America urgently needs renewed leadership on this issue from Congress, the President, and the agencies, as well as state and local governments.

It is important to have a public dialogue about this vital issue. I would like to thank the Committee for having this hearing to facilitate that essential dialogue. I look forward to working with you and am happy to answer any questions you may have.

ARNOLD & PORTER LLP

Jeffrey H. Smith
Jeffrey.Smith@aporter.com

202.942.5115
202.942.5999 Fax
202.468.4495 Cell

555 Twelfth Street, NW
Washington, DC 20004-1206

August 5, 2008

The Honorable Joseph Lieberman
Chairman
Committee on Homeland Security and Governmental Affairs
340 Dirksen Building
Washington, DC 20510

Dear Mr. Chairman:

When I testified on July 23 at the Committee's hearing on information sharing, you asked about the recommendation on "authorized uses" made by the Markle Task Force on National Security in the Information Age.

Although I hope I answered your question in the hearing, some discussion on the subject ensued between the Committee and the panel. Therefore, I thought you and the Committee might be interested in the attached memorandum that explains more fully the recommendation of the Task Force. We believe that, if adopted, the authorized use standard would improve the sharing, use and protection of critical information while protecting civil liberties.

I hope you find this memorandum to be of value and please let me know if the Task Force or I can be of any further assistance. And, thank you again for the opportunity to testify on this very important subject.

Best regards,

Jeffrey H. Smith

Enclosure

Mobilizing Information to Prevent Terrorism
Accelerating Development of a Trusted Information Sharing Environment

Authorized Uses to Streamline and Legitimize Information Sharing

Current distinctions of intelligence information are outdated and confusing and stand in the way of trusted information sharing. In its July 2006 Report, the Markle Task Force on National Security in the Information Age[1] recommends a new "authorized use" standard for government handling of legally collected information. Authorization to access and share information is based on a standard for how the information is going to be used, rather than on the nationality of the subject or the location of the collection. This standard would improve the sharing, use and protection of relevant terrorism information while protecting civil liberties.

The U.S. Persons and the "Line at the Border" rules must be updated to current threat and technologies

At least since the late 1970s, access to, and sharing of, intelligence information collected by U.S.government agencies have been controlled in significant measure by two factors:

(1) Whether or not such information was collected within U.S. territory or overseas; and
(2) Whether or not such information included information pertaining to US Persons.

Under these rules, US government agencies have treated information regarding US Persons more carefully than information concerning non-US Persons, and the government has applied much higher standards to the sharing of information collected inside the US, particularly information collected through sensitive methods such as electronic surveillance, than to information collected outside the US.

The values these rules represent must continue to be respected. U.S. persons must continue to be protected from unreasonable intrusion and unjustified actions by U.S. government agencies.

Yet, over time, these rules have become subject to:

- Over-Interpretation: The rules on access to and sharing of information have been over-interpreted, and misinterpreted, well beyond their original scope and purposes. This is often due to a combination of complexity, uncertainty, bureaucratic rigidity and turf-protection;

- Technological Change: The evolution in global communications (particularly the Internet) and the borderless nature of post-9/11 threats have rendered these place-of-collection and

[1] The Task Force was founded in the aftermath of the September 11 attacks and is a distinguished, bi-partisan group of the nation's foremost national security experts from the administrations of Presidents Carter, Reagan, George H.W. Bush, Clinton, and George W. Bush, as well as leaders in the field of technology and civil liberties.

US Person status distinctions, as a basis of controlling access to, and sharing of, intelligence information no longer workable.

The Current Situation: The government lacks clear and consistently interpreted rules for accessing and sharing information that are adapted to the current threat and technology environment. As a result, government officials too often:

- fail to share information at all (due to risk-aversion);
- engage in ad hoc sharing practices without adequate regard for civil liberties; or
- undertake uncoordinated collection activities outside their defined missions.

These rules must be adjusted in the post 9/11 world.

It is imperative for the sharing of legally collected information that the U.S. persons rule be replaced with clear procedures that support increased sharing while continuing to protect civil liberties. The procedures require that we:

- Develop and issue new guidelines and rules for information access and sharing on the purpose for which the party seeking access intends to use the information.
    - These guidelines for authorized use access and sharing should be based on the legal authorities for and specific mission of each agency. They should reflect the sensitivity of the information and how the receiving official will use it.
    - Authorized uses should be mission- or threat-based justifications to demonstrate that information was accessed or shared for a reason that the government has determined beforehand to be appropriate and allowable. In most cases, predetermined authorized uses would not apply to individual information items but, rather, to categories or types of information.
- Build an efficient oversight and technology system that enables users to select, articulate, and electronically certify an "authorized use" as the basis for their access to information.
- Mitigate risk aversion by establishing carefully considered "safe harbor" protections to ensure that, so long as there is a record of a proper authorized use having been articulated simultaneously with information access or sharing, and so long as there is no indication of bad faith, no punitive action could be taken against an individual government officer for having shared information with another agency.
- Establish a government-wide dispute resolution mechanism for information sharing conflicts.
- Implement audit-logs to monitor use and compliance of procedures and rules.

To achieve the widest consensus for implementation, there should be an open debate involving the Executive Branch, Congress, and the general public resulting in clear and appropriate guidelines.

GENERAL PRINCIPLES FOR DEVELOPING THE AUTHORIZED USE STANDARD

Ensure Applicability Across the Government. Generally speaking, categories of authorized use should apply to all information sharing environment components, although, as discussed elsewhere in this report, the guidelines will also have to be tailored to the specific missions and authorities of individual departments and agencies.

Tailor to Anticipated Uses. The authorized use standard for access to, or sharing of, information generally should be lower when the information is to be used for terrorism-related analysis, policymaking, or alerting functions; and higher when the anticipated authorized use is reasonably expected to include some action (such as detention, travel restrictions, or denial of a benefit) within the territory of the United States or against U.S. Persons.

Treat Anonymized Information Differently. The Task Force has recommended the use of anonymization technology to enable information analysis without disclosure of personally-identifiable information. When combined with anonymization techniques, the implementation of a properly-defined and implemented authorized use system could facilitate use of information in ways that enhance both national security and the protection of civil liberties. For example, if an agency has an authorized use to obtain only a few records in a large dataset, the overall information could be correlated anonymously to determine the finite number of matching records. The receiving agency could use the matches discovered in the anonymized information to request specific records for sharing only when it meets a higher threshold of justification. This not only has obvious civil liberties benefits, but also would contribute to operational efficiency (i.e., less information transferred means less information to keep current).

Articulate Authorized Use Guidelines. Authorized use guidelines should be developed through an appropriate public process. Legislation would set out the framework for an authorized use regime and the Executive Branch would develop specific implementations through a formal high-level process with as much transparency as possible. This process should include the participating agency's information sharing environment privacy and civil liberties officer, and should be reviewed by the Privacy and Civil Liberties Oversight Board prior to final approval by the President. Expansions to an authorized use should receive a thorough review and specific approval that is made public.

Electronic Record of Authorized Uses and Compliance Monitoring Through Audits. Transmitting agencies would be required to keep an auditable record of each dissemination for which an articulation of an authorized use was made. The sharing and subsequent use of the information would be subjected to auditing and monitoring of compliance to ensure that information is utilized consistently with authorized uses. This auditing will be helpful to protecting civil liberties, as well as the security of information against insider compromise. Auditing monitoring sharing logs would have the added benefit of creating new intelligence and knowledge for analysts, policymakers, and others, as well as facilitating dispute resolution, by creating real-time, electronically-accessible records that automated software could use to identify common questions by different analysts. Such real-time logs will also play a role in helping identify unauthorized access, both for counter-intelligence purposes and to protect civil liberties.

Minimize Transaction Costs. The system must be designed from the outset to record authorized uses electronically in the simplest possible way consistent with the sensitivity of the information requested. Sometimes it will be automatic, such as when an entire agency or component is authorized to receive information based on its mission. Other times it will require a single mouse click or a short explanation where an officer receiving, forwarding or authorizing access to information must affirmatively articulate an authorized use. To the extent that this process can be electronic—which we strongly recommend as the preferred solution wherever possible—it will minimize transaction costs to users. It will be critical, however, that, as the government seeks to minimize transaction costs for articulating authorized uses, it also creates mechanisms to ensure that authorized use determinations do not become either arbitrary or automatic. Officers must be required to think through, albeit quickly, their selections, and be able to articulate why they selected the authorized use they did.

Clarify Roles and Responsibilities. It is important to clarify the roles and responsibilities of all participants in the information sharing environment. Implementation of authorized uses will help ensure that departments and agencies stay in their lanes, as authorized by our nation's leadership and understood by the public.

United States Government Accountability Office
Washington, DC 20548

August 28, 2008

The Honorable Joseph I. Lieberman
Chairman
Committee on Homeland Security and Governmental Affairs
United States Senate

The Honorable George V. Voinovich
Ranking Member
Subcommittee on Oversight of Government Management,
the Federal Workforce and the District of Columbia
Committee on Homeland Security and Governmental Affairs
United States Senate

Subject: *Information Sharing: Questions for the Record Regarding Security Clearances for State and Local Officials*

On July 23, 2008, I testified before your committee at a hearing on Information Sharing.[1] This letter responds to two questions for the record you posed. Your questions and my responses follow.

1. **As you may know, Senator Akaka and I have been working to remove the Department of Defense security clearance process from the Government Accountability Office's (GAO) high risk list by lessening the amount of time it takes to investigate and adjudicate security clearances and by ensuring that Federal agencies recognize security clearances granted by other Federal agencies. Has GAO investigated how long it is taking Federal agencies to grant State and local officials security clearances?**

In our October 2007 report on state and local fusion centers,[2] we reported on Department of Homeland Security (DHS) and Federal Bureau of Investigation (FBI) goals for processing security clearances for state and local officials.[3] With respect to security clearances, we reported that DHS set a goal of 90 days to complete a Secret clearance, and FBI set a goal of 45 to 60 days to complete a Secret clearance and 6 to 9 months to complete a Top Secret clearance. We also reported on average

[1]GAO, *Information Sharing: Definition of the Results to be Achieved in Terrorism-Related Information Sharing Is Needed to Guide Implementation and Assess Progress*, GAO-08-637T (Washington, D.C.: July 23, 2008).
[2]GAO, *Homeland Security: Federal Efforts Are Helping to Alleviate Some Challenges Encountered by State and Local Information Fusion Centers*, GAO-08-35 (Washington, D.C.: Oct. 30, 2007).
[3]While some fusion centers may have representatives from the National Guard participate in their centers, the Department of Defense is not involved in granting fusion center staff security clearances.

processing time the FBI reported taking to reduce the turnaround time for clearances. According to the FBI, Top Secret security clearances granted by the FBI to state and local personnel in March 2007 took an average of 63 days to complete, down from an average of 116 days in fiscal year 2006.

2. What are your thoughts on what obstacles exist to having Federal agencies recognize security clearances granted to State and local officials by other agencies?

In our October 2007 report on state and local fusion centers,[4] we identified challenges that state and local officials reported related to obtaining and using security clearances provided by DHS and the FBI. Specifically, officials at 19 of the 58 fusion centers we contacted cited difficulties with federal agencies, particularly DHS and the FBI accepting each other's clearances. We reported that this lack of reciprocity could hinder the centers' ability to access facilities, computer systems, and information from multiple agencies. We also reported that DHS and Department of Justice (DOJ) officials said that they were not aware of fusion centers encountering challenges with reciprocity of security clearances, but that there were complications in the clearance process. Specifically, these officials reported on complications such as multiple federal agencies carrying out their own clearance processes and granting clearances without coordinating with each other; differences in standards for obtaining a clearance, such as requiring a polygraph examination to obtain a clearance; and the overall lack of a consolidated system, or efforts to develop one, for managing security clearances.

Eileen R. Larence

Eileen R. Larence
Director, Homeland Security and Justice Issues

[4]See GAO-08-35.

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
PROGRAM MANAGER, INFORMATION SHARING ENVIRONMENT
WASHINGTON, DC 20511

August 27, 2008

The Honorable Joseph I. Lieberman
Chairman
Committee on Homeland Security and Governmental Affairs
United States Senate
Washington, DC 20510-6250

Dear Mr. Chairman:

Thank you for your August 13, 2008 letter containing questions in relation to the July 23, 2008 hearing, titled "Information sharing: Connecting the Dots at the Federal, State, and Local levels." This letter responds to the following post-hearing question for the record regarding the implementation of Section 210(a) of P.L. 110-53:

The 9/11 Commission Act of 2007 includes a section that gives agencies the authority to consider "the success of an employee in appropriately sharing information" when providing monetary incentives and cash awards to federal employees. What is being done within federal agencies to implement this provision and provide direct monetary incentives to employees who effectively promote and engage in information sharing?

Fostering an information sharing culture is the most formidable challenge confronting the Information Sharing Environment (ISE). In the post-9/11 world, a predisposition to share the right information with those who need it is not merely optional, but fundamental, firmly grounded in law and regulation. ISE cultural change initiatives aim to ensure that this is clearly understood and that managers are held accountable for driving changes in information management that encourage and advance the ISE in their agencies.

As part of our performance management requirements under Section 1016 of the Intelligence Reform and Terrorism Prevention Act, we conducted a Spring 2008 performance assessment, which surveyed Information Sharing Council (ISC) member agencies on their adoption of incentives to promote a culture of information sharing. In response to our inquiry, five ISC agencies reported that they direct monetary incentives to employees who effectively promote and engage in information sharing. These agencies, and descriptions of their initiatives, are as follows:

- **Department of Defense - Joint Chiefs of Staff (JCS):** The JCS has recently allowed employees to receive a **cash award** for recognition of their information sharing activities.

- **Department of Energy (DOE)**: For relevant personnel who have information sharing performance evaluation elements in their performance appraisals, DOE awards a **performance bonus** where appropriate.

- **Department of Homeland Security - Customs and Border Protection (CBP):** When an individual posing a national security threat has been identified, and the identification was a product of information sharing, leading to the apprehension, inadmissibility, or detention of a subject with terrorist ties, the officers associated with the event may receive a **cash award.**

- **Department of Transportation (DOT)**: The Intelligence Division of the Office of Intelligence, Security and Emergency Response has incorporated information sharing into division members' performance appraisals and provided **monetary bonuses** to the division members for their enthusiastic support to all matters relevant to information sharing.

- **National Counter Terrorism Center (NCTC): Monetary incentives** for employees who effectively promote and engage in information sharing are part of the evaluation and compensation system.

In addition to monetary incentives, many agencies such as DOE, DOT, and ODNI have put information sharing into their performance appraisals. For example, the ODNI includes collaboration and engagement as one of the performance elements in all ODNI performance appraisals. As the IC moves to a single appraisal system, an information-sharing performance element will be mandated for all IC agencies.

While ISC member agencies have made considerable progress to foster an information sharing culture, my office continues to press ahead with our efforts to further advance these initiatives across the ISE. Accordingly, in July 2008, we collaborated with the Office of Personnel Management to provide guidance to all ISC member agencies to incorporate information sharing elements in employee performance appraisals. We will measure the success of this guidance during our Fall 2008 performance assessment and will collect fact-based data to support decisions and report progress against this initiative.

I very much appreciate your interest in helping my office to promote an information sharing culture among ISE partners.

Sincerely,

Thomas E. McNamara

Question#:	1
Topic:	security clearance process
Hearing:	Information Sharing: Connecting the Dots at the Federal, State, and Local Levels
Primary:	The Honorable George V. Voinovich
Committee:	HOMELAND SECURITY (SENATE)

Post-Hearing Questions for the Record
Submitted to Charles E. Allen

Question: As you may know, Senator Akaka and I have been working to remove the Department of Defense security clearance process from the Government Accountability Office's (GAO) high risk list by lessening the amount of time it takes to investigate and adjudicate security clearances and by ensuring that Federal agencies recognize security clearances granted by other Federal agencies. On average, how long does it take the Department of Homeland Security (DHS) to grant State and local officials secret and top secret security clearances?

Answer: Interim Security Clearances at the Secret level are granted within one (1) week of receipt of the required documentation from the applicant. The issuance of the Final Secret or Top Secret Clearance is dependent upon the completion of the investigation from OPM which takes on average 54 days. The final adjudication is completed within 30 days after receipt of the final report of the investigation from OPM.

Question:
In what instances does DHS not recognize a security clearance granted to a State or local official by another Federal agency?

Answer: DHS accepts security clearances under reciprocity, as long as the clearance was granted according to Federal standards and is at the level required for the position. Federal agencies are required to record active security clearance information in the Central Verification System (CVS) or the Department of Defense (DoD) Joint Personnel Adjudication System (JPAS). We check the CVS and JPAS for individuals requiring a security clearance to work for or with DHS. If the individual does not have a security clearance or a higher level clearance is required, we initiate the background investigation.

This process applies to Federal employees and contractor personnel, as well as State and local officials requiring a security clearance to work with DHS.

Question:
In what instances does DHS recognize a security clearance granted to a State or local official by another Federal agency without additional investigation or adjudication by DHS?

Answer: As noted above, an investigation is only needed when the individual does not have a security clearance or requires a higher level security clearance. When the investigation is completed, we adjudicate the results and determine the person's eligibility for a security clearance.

Question:
In what instances does DHS recognize a security clearance granted to a Federal employee by another Federal agency without additional investigation or adjudication by DHS?

Question#:	2
Topic:	incentives
Hearing:	Information Sharing: Connecting the Dots at the Federal, State, and Local Levels
Primary:	The Honorable Joseph I. Lieberman
Committee:	HOMELAND SECURITY (SENATE)

Question: The 9/11 Commission Act of 2007 includes a section that gives agencies the authority to consider "the success of an employee in appropriately sharing information" when providing monetary incentives and cash awards to federal employees." What is being done within DHS to implement this provision and provide direct monetary incentives to employees who effectively promote and engage in information sharing?

Answer: DHS will consider a reward program proposal at the next quarterly meeting of its Information Sharing Governance Board (ISGB), in September. The ISGB is the principal-level steering committee and decision-making body for all Departmental information sharing and collaboration issues and activities. The proposal contemplates varying levels of formal recognition that correspond to the degree of individual accomplishment achieved. The complete spectrum of potential rewards or incentives is likely to range from the awarding of certificates for outstanding performance on a quarterly basis (with corresponding impact upon that individual's annual performance appraisal) to annual recognition for honorary achievement, including the "Outstanding Information Sharing Medal," which is accompanied by a cash or leave award.

Question#:	3
Topic:	SIPRnet
Hearing:	Information Sharing: Connecting the Dots at the Federal, State, and Local Levels
Primary:	The Honorable Joseph I. Lieberman
Committee:	HOMELAND SECURITY (SENATE)

Question: In July 2007 your office asked the Department of Defense to work with DHS to find a way for cleared state and local officials to have access to SIPRNet, DOD's main secret level network. DHS has told the Committee that DOD has been reluctant to provide them with access. This means that many cleared state and local officials lack access to important intelligence sites run by the CIA, the National Geospatial Intelligence Agency, and NORTHCOM. Please discuss what is being done to resolve this issue and address this information sharing gap.

Answer: DHS has worked with DOD officials in an attempt to provide an acceptable level of SIPRNet access to appropriately cleared State and local officials, with a valid need for access to relevant information, in the performance of their respective missions. As a part of this effort, we have exchanged correspondence and held numerous meetings with DOD, including at the principal and staff levels within the Offices of the Under Secretary of Defense for Intelligence (USDI); the Assistant Secretary-Networks and Information Integration (ASD-NII); the Assistant Secretary-Homeland Defense (ASD-HD); and the Joint Staff. To date, we believe we have satisfactorily addressed access control and capacity concerns originally presented by DOD, and have answered any and all other questions raised.

In April 2008, Paul McHale, the Assistant Secretary of Defense for Homeland Defense and Americas Security Affairs, and Charles Allen, Undersecretary of Homeland Security for Intelligence and Analysis (I&A), agreed to work in concert to achieve appropriate, agile access to SIPR data holdings through the DHS Homeland Secure Data Network. And in September 2008, DHS and ASD-HD have proposed a phased approach that would allow State and local officials' access to specifically identified SIPRNet sites. This recommended approach, which will provide initial access to NORTHCOM and a limited number of other SIPRNet sites, has been endorsed by DHS I&A management and is currently in staffing in DOD. Assuming approval by DOD authorities, the initial phase is expected to be implemented in the First Quarter of FY 2009, and we have identified key stakeholders from 24 State and Local Fusion Centers (SLFCs) as participants. We understand that the DOD plan also describes an additional phase that consists of enforcing a policy that custodians of SIPRNet-hosted information resources are responsible for implementing any appropriate access limitations locally, while access to the SIPRNet will be permitted for all Federally Secret-cleared personnel.

It is important to note that neither DHS nor DOD are the final authorities regarding the access to all data resident on SIPRNet. In the examples referenced in the question, two of the providers cited – the CIA and the National Geospatial Agency – release authority rests with the Agency directors and the Director of National Intelligence. DHS will work with these entities, in concert with the Director of National Intelligence and the Office of the Program Manager – Information Sharing Environment (PM-ISE), to ensure appropriate access.

○