AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

DEPARTMENT OF HOMELAND SECURITY'S INFORMATION ANALYSIS AND INFRASTRUCTURE PROTECTION BUDGET PROPOSAL FOR FISCAL YEAR 2005

JOINT HEARING

OF THE

SUBCOMMITTEE ON INTELLIGENCE AND COUNTERTERRORISM

AND

SUBCOMMITTEE ON INFRASTRUCTURE AND BORDER SECURITY

BEFORE THE

SELECT COMMITTEE ON HOMELAND SECURITY
HOUSE OF REPRESENTATIVES

ONE HUNDRED EIGHTH CONGRESS

SECOND SESSION

MARCH 4, 2004

Serial No. 108–39

Printed for the use of the Select Committee on Homeland Security

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

U.S. GOVERNMENT PRINTING OFFICE

22–589 PDF WASHINGTON : 2005

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

SELECT COMMITTEE ON HOMELAND SECURITY

CHRISTOPHER COX, California, *Chairman*

JENNIFER DUNN, Washington
C.W. BILL YOUNG, Florida
DON YOUNG, Alaska
F. JAMES SENSENBRENNER, JR., Wisconsin
W.J. (BILLY) TAUZIN, Louisiana
DAVID DREIER, California
DUNCAN HUNTER, California
HAROLD ROGERS, Kentucky
SHERWOOD BOEHLERT, New York
LAMAR S. SMITH, Texas
CURT WELDON, Pennsylvania
CHRISTOPHER SHAYS, Connecticut
PORTER J. GOSS, Florida
DAVE CAMP, Michigan
LINCOLN DIAZ–BALART, Florida
BOB GOODLATTE, Virginia
ERNEST J. ISTOOK, JR., Oklahoma
PETER T. KING, New York
JOHN LINDER, Georgia
JOHN B. SHADEGG, Arizona
MARK E. SOUDER, Indiana
MAC THORNBERRY, Texas
JIM GIBBONS, Nevada
KAY GRANGER, Texas
PETE SESSIONS, Texas
JOHN E. SWEENEY, New York

JIM TURNER, Texas, *Ranking Member*
BENNIE G. THOMPSON, Mississippi
LORETTA SANCHEZ, California
EDWARD J. MARKEY, Massachusetts
NORMAN D. DICKS, Washington
BARNEY FRANK, Massachusetts
JANE HARMAN, California
BENJAMIN L. CARDIN, Maryland
LOUISE MCINTOSH SLAUGHTER, New York
PETER A. DEFAZIO, Oregon
NITA M. LOWEY, New York
ROBERT E. ANDREWS, New Jersey
ELEANOR HOLMES NORTON, District of Columbia
ZOE LOFGREN, California
KAREN MCCARTHY, Missouri
SHEILA JACKSON-LEE, Texas
BILL PASCRELL, JR., North Carolina
DONNA M. CHRISTENSEN, U.S. Virgin Islands
BOB ETHERIDGE, North Carolina
KEN LUCAS, Kentucky
JAMES R. LANGEVIN, Rhode Island
KENDRICK B. MEEK, Florida

JOHN GANNON, *Chief of Staff*
STEPHEN DEVINE, *Deputy Staff Director and General Counsel*
THOMAS DILENGE, *Chief Counsel and Policy Director*
DAVID H. SCHANZER, *Democrat Staff Director*
MARK T. MAGEE, *Democrat Deputy Staff Director*
MICHAEL S. TWINCHEK, *Chief Clerk*

Subcommittee on Intelligence and Counterterrorism

Jim Gibbons, Nevada, *Chairman*

John Sweeney, New York, *Vice Chairman*
Jennifer Dunn, Washington
C.W. Bill Young, Florida
Harold Rogers, Kentucky
Christopher Shays, Connecticut
Lamar Smith, Texas
Porter Goss, Florida
Peter King, New York
John Linder, Georgia
John Shadegg, Arizona
Mac Thornberry, Texas
Christopher Cox, California, *Ex Officio*

Karen McCarthy, Missouri
Edward J. Markey, Massachusetts
Norman D. Dicks, Washington
Barney Frank, Massachusetts
Jane Harman, California
Nita M. Lowey, New York
Robert E. Andrews, New Jersey
Eleanor Holmes Norton, District of Columbia
James R. Langevin, Rhode Island
Kendrick B. Meek, Florida
Jim Turner, Texas, *Ex Officio*

Subcommittee on Infrastructure and Border Security

Dave Camp, Michigan, *Chairman*

Kay Granger, Texas, *Vice Chairwoman*
Jennifer Dunn, Washington
Don Young, Alaska
Duncan Hunter, California
Lamar Smith, Texas
Lincoln Diaz-Balart, Florida
Robert W. Goodlatte, Virginia
Ernest Istook, Oklahoma
John Shadegg, Arizona
Mark Souder, Indiana
John Sweeney, New York
Christopher Cox, California, *Ex Officio*

Loretta Sanchez, California
Edward J. Markey, Massachusetts
Norman D. Dicks, Washington
Barney Frank, Massachusetts
Benjamin L. Cardin, Maryland
Louise McIntosh Slaughter, New York
Peter A. DeFazio, Oregon
Sheila Jackson-Lee, Texas
Bill Pascrell, Jr., New Jersey
Charles Gonzalez, Texas
Jim Turner, Texas, *Ex Officio*

CONTENTS

Page

STATEMENTS

The Honorable Dave Camp, a Representative in Congress From the State of Michigan, and Chairman, Subcommittee on Infrastructure and Border Security 32
The Honorable Loretta Sanchez, a Representative in Congress From the State of California, and Ranking Member, Subcommittee on Infrastructure and Border Security 4
The Honorable Jim Gibbons, a Representative in Congress From the State of Nevada, and Chairman, Subcommittee on Intelligence and Counterrorism 1
The Honorable Karen McCarthy, a Representative in Congress From the State of Missouri, Ranking Member, Subcommittee on Intelligence and Counterrorism 2
The Honorable Christopher Cox, a Representative in Congress From the State of California, and Chairman, Select Committee on Homeland Security 26
The Honorable Jim Turner, a Representative in Congress From the State of Texas, Ranking Member, Select Committee on Homeland Security 6
The Honorable Robert E. Andrews, a Representative in Congress From the State of New Jersey 35
The Honorable Norman D. Dicks, a Representative in Congress From the State of Washington 45
The Honorable James R. Langevin, a Representative in Congress From the State of Rhode Island 61
The Honorable Sheila Jackson-Lee, a Representative in Congress From the State of Texas
Prepared Statement 8
The Honorable John Shadegg, a Representative in Congress From the State of Arizona 37
The Honorable Christopher Shays, a Representative in Congress From the State Connecticut 32
The Honorable Louise McIntosh Slaughter, a Representative in Congress From the State of New York 8
The Honorable John E. Sweeney, a Representative in Congress From the State of New York 44

WITNESS

General Libutti, Under Secretary, Information Analysis and Infrastructure Proection, Department of Homeland Security
Oral Statement 10
Prepared Statement 13

APPENDIX

Material Submitted for the Record

Questions Submitted from the Honorable James R. Langevin 61
Questions Submitted from the Honorable Sheila Jackson-Lee 56
Questions Submitted from the Honorable John Shadegg 49
Questions Submitted from the Hororable Mac Thornberry 50

THE DEPARTMENT OF HOMELAND SECURITY'S INFORMATION ANALYSIS AND INFRASTRUCTURE PROTECTION BUDGET PROPOSAL FOR FISCAL YEAR 2005

Thursday, March 4, 2004

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON INTELLIGENCE
AND COUNTERTERRORISM,
AND
SUBCOMMITTEE ON INFRASTRUCTURE
AND BORDER SECURITY,
SELECT COMMITTEE ON HOMELAND SECURITY,
Washington, DC.

The joint subcommittee met, pursuant to call, at 10:00 a.m., in Room 2318, Rayburn House Office Building, Hon. Jim Gibbons presiding.

Present: Representatives Gibbons, Camp, Shays, Shadegg, Sweeney, Cox (Ex Officio), McCarthy, Sanchez, Markey, Dicks, Slaughter, Andrews, Pascrell, Langevin and Turner (Ex Officio).

Mr. GIBBONS. I see that a quorum is present. The Subcommittee on Intelligence and Counterterrorism and the Subcommittee on Infrastructure and Border Security will come to order.

The subcommittees are meeting jointly today to hear testimony on the Department of Homeland Security's proposed fiscal year 2005 budget for information analysis and infrastructure protection. Let me indicate that I will be chairing the first part of this hearing and that Chairman Dave Camp will be chairing the second half after he wraps up some other additional important work that he has over at the Ways and Means Committee.

I would ask unanimous consent that members' statements be included in the hearing record and encourage members of the subcommittees to submit their opening statements for the record.

I now recognize myself for an opening statement.

Under Secretary Libutti, thank you for being here today. I would like to start by commending you on your hard work and dedication to protecting our homeland and preserving our freedoms. You have had and continue to have a difficult and complex task.

Today's hearing is part of a series focusing on various aspects of the Department of Homeland Security's budget submission for fiscal year 2005. Today we are here to, first, review the 2005 budget plans for the IAIP or Information Analysis and Infrastructure Protection; second, to ensure that the Department is making optimal progress and fulfilling its responsibilities under the Homeland

Security Act and; finally, to examine the directorate's concurrent initiatives and future plans.

The Information Analysis and Infrastructure Protection piece of the budget accounts for $864 million of the Department's $33.8 billion budget. This represents an increase of $30.2 million over the fiscal 2004 budget enacted levels.

One of the principal objectives behind the Department of Homeland Security is to facilitate the analysis of threats against the homeland and for future acts of terrorism; and IAIP is the very core of this capability. The IAIP Directorate is charged with identifying and assessing current and future threats to the homeland, mapping those threats against our vulnerabilities, issuing timely warnings and taking action to protect the U.S. homeland. This is a long-term project with long-term implications for America's security.

While the Department is continuing to focus on our long-term needs, the Terrorist Threat Integration Center is working with the Department to compile all-source intelligence and distribute information in a timely manner. The Department of Homeland Security must be a full partner in this endeavor, and I know we are all interested in hearing how your relationship with TTIC is progressing.

As part of your opening statement, I appreciate it if you would speak to the relationship with TTIC along with how the recently announced Homeland Security Information Network will interact with TTIC and the Homeland Security Operations Center.

It is important, as we conduct our oversight responsibilities over the Department that Congress continues to provide you with the resources and legal authorization you need to secure and defend America, and that is why we are here today. I look forward to hearing your comments.

The chairman will now recognize the ranking member of the Subcommittee on Intelligence and Counterterrorism, Ms. McCarthy of Missouri, for her opening statement. Ms. McCarthy.

Ms. MCCARTHY. Thank you, Mr. Chairman; and I would request that members who arrive before Mr. Libutti begins his testimony be able to speak.

Mr. GIBBONS. The chairman sees no problem with that, so long as they recognize that the committee's standards are that they have opportunity for an opening statement, which if they don't present an opening statement that time will be included in their time for questioning.

Ms. MCCARTHY. Yes, sir. I appreciate that, Mr. Chairman. I thank you, and I thank the Secretary.

We are pleased that you are here, and we are anxious for you to take us through the $865 million budget submission for Information Analysis and Infrastructure Protection Directorate. As ranking member, Jim Turner, has noticed in recent statements, the Directorate's real-time ability to assess threats to the homeland and identify existing vulnerabilities in our infrastructure is an area we would like you to speak to this morning.

We are interested in hearing about ongoing efforts to improve the depth and breadth of intelligence analysis at the Directorate as well as the connectivity among all key units across government doing similar analysis.

Where are the existing gaps and weaknesses? What can our committee do to help your leadership solve these problems rapidly in authorizing legislation that we expect to pass and enact later this year? And what is the time frame within the coming fiscal year for showing results?

Hopefully, you will cover all of this ground this morning.

Mr. Secretary, it would also be my hope that you cast light on what is being done to speed the issuing of information warnings and advisories to State and local officials and to improve the quality of those communications so that businesses, schools, churches and families across America have the best guidance in hand from the Federal Government when the threat level rises.

Secretary Ridge's announcement last week of a new initiative, the Homeland Security Information Network, hits us in the right direction by creating a comprehensive, computer-based counter-terrorism communication system in all the 50 States and the 50 major urban areas.

The Department has the right idea to strengthen the quality and flow of threat information, and now we have to assure that that is sufficient and that there is follow-through.

If there is one universality from constituent groups that I hear from, it is the need for the DHS to provide timely and actionable information sharing between Federal agencies and State and local agencies. They look to the Department for reliable and accurate information concerning terrorist threats in local communities all across our country.

Tim Daniel, the Director of the State of Missouri Office of Homeland Security, tells me that information sharing needs to go both ways. When Missouri State and local officials have information concerning possible terrorist activities, they need to know not only who to contact at the Federal level but also that their State information will be considered in a timely way.

The feedback loop is still under construction, and I would welcome your wisdom, Mr. Secretary, on how best to complete this loop.

Since we are primarily focused today on dissecting the budget, it would be helpful to have a clear understanding of how many dollars are dedicated toward information sharing with localities and communities. The Homeland Security Operations Center is receiving a big plus up of funds, $10 million, in part to undergird the implementation of national systems for information sharing, and I would appreciate you sharing with this committee a Directorate-wide breakdown of how funds are actually expended for information sharing purposes.

It would also be useful to hear a broader explanation of where and how time is lost in the process of forwarding important real-time intelligence threat information to first responders. The first responders in the Fifth District of Missouri and all around the U.S. need timely and actionable information from the Federal Government.

Mr. Secretary, share your plans on enhancing communication at all levels and working to provide our local communities with the resources they need to respond in emergency situations. I hope you

will provide more information on this topic so the committee has a better sense of how to fix this nationwide dilemma.

A separate policy matter slow to develop involves IAIP information analysis and completing that comprehensive threat and vulnerability assessment and to guide spending priorities. In releasing our one-year anniversary report last week, the committee emphasized the need to have this blueprint in place, regardless of the cost, by October 1 of this year; and I would simply like to reiterate that point with you, our distinguished panelist. How realistic is that goal, Mr. Secretary?

Let me close by emphasizing the deep appreciation I have for the work you are doing, Mr. Secretary. Protecting the homeland is a mammoth responsibility, given the many different avenues that exist for attacking our infrastructure, but we are supportive of your intentions, efforts and long-term goals and will continue as a good-faith partner in helping you close the security gaps facing our Nation and communities.

Thank you, Mr. Chairman, I yield back.

Mr. GIBBONS. Thank you, Ms. McCarthy.

The Chair recognizes once again that the chairman of the Subcommittee on Infrastructure and Border Security will submit his opening remarks for the record.

Mr. GIBBONS. We would now turn to the ranking minority member of the Subcommittee on Infrastructure and Border Security, Ms. Sanchez of California, for her opening remarks.

Ms. SANCHEZ. Thank you, Mr. Chairman, and thank you, Mr. Secretary, for appearing before us today.

Because of the broad scope of the IAIP Directorate, I am pleased that both the members of the Intelligence and Counterterrorism and the Infrastructure and Border Security Subcommittees are here today. You probably have one of the most difficult charges in the whole area of homeland security, but a lot of us don't have a very good idea of how you are structured and what is going on and what you are really doing, and I think that is one of the reasons why you are here before us today, because we are trying to find some answers.

To date, we still don't have a comprehensive study of the Nation's critical infrastructure to determine where our weaknesses lie, and I think that only after such an assessment can we really, as Members of Congress, decide how to put priorities forward and where to put the resources that we need so that we can ensure that chemical plants and electrical grids and water treatment plants and all our other critical infrastructure is protected.

You can imagine how disappointed I am to see in the budget there are only two areas in your Directorate that experience a cut in funding this year, and that would be the threat—from the levels of last year, and that would be threat determination and assessment of $6.3 million and infrastructure vulnerability and risk assessment, $12.6 million. Yet, at the same time, the Homeland Security Department says that it will have a database with a prioritized list of critical infrastructure by the end of this year.

The last time that I spoke with Robert Liscouski, the Assistant Secretary For Infrastructure Protection who works for you, he told me that he would be surprised if a risk assessment could be done

within 5 years. That is what he said in front of our subcommittee. That time I and other members of the subcommittee impressed upon him the seriousness and the importance of the endeavor, because I do believe that it is really the beginning of what we need in order for us to do our job to commit—and I told him to please commit resources and personnel to get that going.

That was last autumn. I would like to hear from you what work is being done on that important issue, and I don't think that we can make correct decisions until we get that done.

It is probably the most important thing you have to do within your Directorate. So, if you are cutting those, do I assume that you don't think it is important? Or do I assume that you think you have enough resources? And if you think you have enough resources, then why over the last year have I been told, oh, it would take 180 days? Oh, what is the start date? We don't know the start date. And then 180 days later I was told, well, it will take—don't even think 5 years will do it. I mean, this is something that I know so many members feel very uncomfortable not having that list of priorities and risks and vulnerability tied into that. So I want to hear from you what is going on with that.

I would also like to hear what kind of capacity and expertise you are building within the Department to assess and protect that critical infrastructure. Who have you hired? Where are they from? What kind of employees are they? Because we really don't know. Are they expert? Are they experts in chemical plants, in electrical grids? I also want to hear how you are working with industry. Because, of course, we all know that probably a little—somewhat over 80 percent of all the critical infrastructure sits in private companies' hands.

I know that you have been sharing with advisory councils and with ISACs, and I know that some of this has been going on even before 9/11, but I want to find out which ones are going well and where we need to help those that are falling behind.

I would also like to know how you work with the ISACs. Do you have people within IAIP responsible for liaison with those groups? Do you give them support and advice? Do you share information? How is information given between the two?

Finally, probably another area of concern that we have is the whole issue of intelligence capabilities. There seems to still be little intelligence capability within DHS, and I know there are some other members that are going to focus on that, so I don't want to go into it.

Like I said, you probably have the toughest job, in my opinion. I know, because I sit on this subcommittee and I think I have one of the toughest jobs trying to get my hands around all of this.

So, as I said, we are trying to figure out how you are set up, who is doing what, how you are working with other groups. So I thank you for being before us. I think we are going to ask some tough questions, but, if we do, it is because we are trying to get the job done.

Thank you.

Mr. GIBBONS. Thank you, Ms. Sanchez.

We will now turn to members that are present here before Secretary Libutti begins and offer them an opportunity in order of appearance on the committee for a 3-minute opening statement.

We will turn to Mr. Shays.

Mr. SHAYS. I will take my 8 minutes, sir, for questioning.

Mr. GIBBONS. We will go to Mr. Turner of Texas.

Mr. TURNER. Thank you, Mr. Chairman.

Welcome, General Libutti. We are pleased to have you here, your first appearance before our committee; and I was pleased to have the opportunity to visit with you in your office several weeks ago. We certainly appreciate the enormity of the task that you have undertaken and the diligence with which you are pursuing the task at hand.

I know we all understand that we created the Department of Homeland Security as a focal point for intelligence analysis so we could do a better job of what we always referred to as connecting the dots. Certainly, as we look back upon the legislation creating the Department, most of us remember the lengthy debate that occurred regarding the creation of what we now call the Information Analysis and Infrastructure Protection Directorate. Specifically, that debate involved what responsibility the new Department and that Directorate would have.

It disturbed many of us on both sides of the aisle when the President decided that the key task of assembling, analyzing and assessing intelligence related to terrorism would be placed outside of the Department in a new entity called the Terrorist Threat Integration Center. That certainly led to confusion among many of us who have been very much committed from the beginning to ensuring that the new Department was the place where this integration process would occur.

So I think it is important that some of your time today, General Libutti, be devoted to explaining to us what you believe to be the merits of the way the threat integration process has been set up as a so-called joint venture between The Department of Homeland Security and other agencies.

We need to know whether the Directorate's intelligence-related duties and responsibilities are still clearly defined and whether there is an effective, functional relationship with that new center and the other components of the intelligence community as well as with your Directorate.

In addition to the intelligence analysis function, IAIP remains a critical part of the Department and a key component of our overall homeland security efforts. Among your duties are identifying and assessing threats, mapping those threats against vulnerabilities, issuing timely warnings, and serving as a conduit of information to and from State and local law enforcement.

In my view, your Directorate could probably be called the nerve center of the Department of Homeland Security, and in many ways the success of your Directorate will determine the success of the entire Department and of the goals that the Congress had in mind when it created that Department.

One of my key concerns, as expressed, and shared by Congresswoman Sanchez, is the progress toward developing this comprehensive threat and vulnerability assessment. Assistant Secretary

Liscouski testified to this committee that that assessment could take up to 5 years. Finishing that task as soon as possible is critical, because right now we feel that we are driving the homeland security budget without a clear roadmap as to where our limited tax dollars should be spent.

I hope, General, in your testimony today that you will help us by clearing up what has been confusing information from various sources about when we can expect the comprehensive, national threat and vulnerability assessment to be completed. If the date you give us is one that you are not satisfied with, advise us as to what we can do to help you to move that date up to an earlier point. If that involves additional funding, I hope you will be forthright with us and give us that information, because I think the Congress—in a bipartisan way—recognizes that when we created the new Department, merging 22 separate preexisting agencies, that the most important contribution that we tried to make to making our Nation more secure was not just in having a massive merger but in doing some things new that we had not done before. One of those on that list was comprehensive national threat and vulnerability assessment. I hope you will give us a date that we can expect the assessment that to be accomplished.

I am also concerned about the progress in developing the Integrated Terrorist Watch List. That task, to me, is one of the most critical elements of our ability to keep terrorists out of this country. Because every activity, whether it is screening people at our airports or at our land borders or reviewing visas by the State Department, all of those activities to be effective have to have access real time to a comprehensive terrorist watch list.

That task has not been completed. As you know, here we are two and a half years after September 11th; and that responsibility has been passed around to various agencies. It finally landed back with the FBI and with the Terrorist Screening Center.

We continue to get different dates. At the beginning of this year, we were told that the task would be completed by March. That did not happen; and, in fact, according to the Department's strategic plan released last week, this task is not to be completed until the end of this year.

I really think that this is unacceptable, and I really to not understand why we have had such a difficult task doing what I think is a very critical and key part of making this country safer.

Last week one official at the Department even suggested in one publication I read that we may not really need to fully integrate the terrorist watch list, which completely baffled me in light of the fact that this has been a high priority for some time.

Another issue that I want to mention is, despite the fact that there is an overall increase in your Directorate's budget as requested by the President, the request for the item called assessments and evaluations decreases in that budget request by $8 million compared with the current year. This I assume is due to the elimination of the Directorate's funding or share of funding to support the Terrorist Threat Integration Center and the Terrorist Screening Center, but I want you, if you will, General, to address this issue, because I worry that when we end the Department's financial contribution to the Terrorist Threat Integration Center we

further distance the Department from that critical role and from a responsibility that clearly in the Department of Homeland Security Act was a responsibility given to the Department.

There are other areas that I hope you will have the opportunity to touch upon regarding your progress in integrating your new hires and detailees into your work.

I know for a period of time your staffing authorization has exceeded the number of staff that you have been able to hire, and I would like to know how you are progressing there.

I would like to also know and have from you a candid assessment of how well the intelligence community is sharing information with you. I frankly believe that in this new era of trying to protect the homeland that we are still sharing classified intelligence as we did during the Cold War, and if you can't tell me today that there are at least four or five top folks in your Department, and you should be one of those, that knows everything that is available regarding threats to this country, I would say that we are still holding that information too tightly.

I have been in briefings before, and I get the impression that, generally, Secretary Ridge is probably told everything, but I am not convinced that others in critical roles such as yours have total access to all of the classified informing that must be shared in order to be sure this country is secure. I would like to have your candid observations with us regarding that classified information sharing and whether or not you think that I am correct or incorrect with regard to that assessment.

I think I speak for all of my colleagues today that we appreciate the good work you do and the progress you are making, and we want to support you to be sure that we all can accomplish the task that we know is so critical.

Thank you.

Mr. GIBBONS. Thank you, Mr. Turner.

We will now turn to members that were here within the 5-minute time limit of the gavel for a 3-minute opening remark. Mr. Andrews of New Jersey.

Mr. ANDREWS. Mr. Chairman, I will pass on the opening statement and reserve questions.

Mr. GIBBONS. Ms. Slaughter.

Ms. SLAUGHTER. I don't have an opening statement, Mr. Chairman. I will reserve for questions.

Mr. GIBBONS. Mr. Pascrell of New Jersey.

Mr. PASCRELL. I will reserve.

PREPARED STATEMENT OF THE HONORABLE SHEILA JACKSON-LEE, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF TEXAS

Mr. Chairman, thank you for your diligence in organizing today's hearing to discuss and analyze the Fiscal Year 2005 Budget submission for the Directorate for Information Analysis and Infrastructure Protection (IAIP), as this portion of our Department of Homeland Security (DHS) is probably one of the most important to our ability to sustain ourselves in the event of a terrorist attack.

Key to our ability to sustain ourselves in the event of a terrorist attack will be the effectiveness of our IAIP to pick up, interpret, analyze, share, and transmit intelligence information to the Department of Homeland Security (DHS) as a whole. Repeatedly, we have seen instances where there has been demonstrated a weakness in our critical infrastructure. The breakdown of the power grid system in areas such as the Great Lakes, Michigan, Ohio, New York City, Ontario, Quebec, Northern New Jersey, Massachusetts, and Connecticut during the blackout of August 14, 2003

is but one example of the need for DHS to do a better job of vulnerability assessment and evaluation. To date, we are not comfortable that this kind of situation won't occur again; yet the President's Fiscal Year 2005 Budget requests show an $8 million decrease from the current year level for the Assessment and Evaluations budget account. In addition, the request shows reduced funding for the Terrorist Threat Integration Center (TTIC) and the Terrorist Screening Center (TSC) totaling $19 million, which translates to a weakening of the Threat Determination/Assessment and Infrastructure Vulnerability & Risk Assessment resources that the Department will have.

Furthermore, DHS is in dire need of improvements in the area of information-sharing. For example, according to a GAO report released two months ago, the Department of Homeland Security's Division of Customs and Border Patrol (CBP) does not have a national system for reporting and analyzing inspection statistics by risk category. Data from some ports are not available by risk level, not uniformly reported, difficult to interpret, and not complete. Furthermore, when GAO contacted ports to obtain these data, basic data on inspections were not readily available. All five ports that gave information on sources of data said they had extracted data from the national Port Tracking System. However, this system did not include information on the number of non-intrusive examinations or physical examinations conducted, according to risk category. Moreover, a CBP headquarters official stated that the data in the Port Tracking System are error prone, including some errors that result from double counting. One port official told us that the Port Tracking System was not suitable for extracting the examination information we had requested, so they had developed a local report to track and report statistics. A March 2003 Treasury Department Inspector General Report found, among other things, that inspection results were not documented in a consistent manner among the ports and examination statistics did not accurately reflect inspection activities.

In the area of bioterrorism and the need to maintain an effective system of information-sharing, Houston has made some progress in improving its readiness. Infectious disease specialists in Houston have formed a Communicable Disease Alert System (CDAS) to help public officials maintain a close eye on the numbers and types of illnesses that turn up in local clinics and emergency departments and to communicate this information to the public rapidly. The chain of information starts with pre-hospital providers such as emergency medical technicians, paramedics and school nurses who watch for suspicious syndromes or spikes in the occurrence of illnesses. Some hospitals and their emergency departments act as sentinels, reporting spikes in illnesses among patients seeking care at their facilities. Each week, Houston infectious disease specialists and infection control practitioners meet to discuss unusual cases of disease and trade notes about occurrences in their respective institutions. The city of Houston and Harris County rank high in their ability to spot unusual disease patterns.

Threat assessment is key to our nation's ability to detect, withstand, and recover from a potential terrorist attack. Therefore, strong personnel in the technical analysis area of infrastructure protection should be a priority over policy development. It is problematic that, in the 2005 Budget request, the Administration seeks authorization for only 225 intelligence analysts compared to 487 policy/program professional staff.

The need to fund improved threat assessment programs and to hire technical analysts to aid individual states and local areas can be found in Houston's drinking water vulnerability. Two-thirds of the drinking water provided to Houston residents comes from the San Jacinto and Trinity Rivers. These rivers are very vulnerable to pathogen and pesticide pollution, among other things. Houston's "Right-to-Know Report" earned a grade of "Poor" for 2000 and "Fair" for 2001. This report included a need for more prominent placement of the mandatory special alert for people who are more vulnerable to particular contaminants. The 2000 report provided a prominent and incorrect description of arsenic's health threat, and both reports offered misleading information about *Cryptosporidium,* which has been found in Houston's source water. This is but a single illustration of the kind of threat and vulnerability assessment that is in dire need of help from DHS. Our distinguished panelist indicates in his testimony that the President, in his Fiscal Year 2005 Budget, requests $11 million to fund a new biosurveillance initiative that purports to provide for "real-time integration of biosurveillance data. I hope that the IAIP will suggest that part of these funds go to helping individual states to strengthen its threat assessment for bioterrorism.

Our panelist today, DHS Under Secretary for the Information Analysis and Infrastructure Protection Section concluded his testimony that "the fiscal year 2005 budget request provides the resources to enable the IAIP Directorate to manage and grow in its mission of securing the homeland."Our need is urgent, so there really

isn't a lot of time to allow for "growing," unfortunately. The Budget requests that are presented to us today suggest that the Administration feels that we have time for "growing." Because the threat is real and emergent, we do not have the luxury of time. Monies available for general purposes must be intelligently allocated to address specific and localized needs.

Mr. Chairman and Ranking Member, I thank you again for your effort and leadership in giving this Subcommittee the opportunity to analyze and comment on this Budget.

Mr. GIBBONS. Very well. We now have before us Under Secretary Libutti. We look forward to your testimony. You are welcome before us today, and the floor is yours, Mr. Under Secretary.

STATEMENT OF GENERAL LIBUTTI, UNDER SECRETARY, INFORMATION ANALYSIS AND INFRASTRUCTURE PROTECTION, DEPARTMENT OF HOMELAND SECURITY

General LIBUTTI. Thank you, sir. Good morning, Chairman Gibbons, Representative McCarthy, Representative Sanchez, Representative Turner, distinguished members of the subcommittee. I am delighted to appear before you today to discuss the President's 2005 budget request for the Department of Homeland Security and my Directorate IAIP.

I am going to pause in my written prep for my oral and say to you all with great respect and admiration—and I mean this very sincerely, dare I go any other direction—the questions that were in opening comments, if I had recorded all of them, would probably be sufficient to both give me an opportunity to share where we are going and also, candidly speaking, answer your questions. I am a bit new to this process, but I have taken a few notes, and I will come back to those, but I would graciously and respectfully ask for those who have made statements to come back at me with your questions so, in a very logical and concise format, I can respond accordingly. I would just ask with all due respect, sir, that we go that way.

Let me continue with my opening statement, please.

IAIP is the focal point for intelligence analysis, infrastructure protection operations and information sharing—let me underscore information sharing-Within the Department. IAIP merges the capability to identify and assess a broad range of intelligence and information concerns which threaten the homeland. We map, as has been pointed out, that information against national vulnerabilities, our critical infrastructure, and we press on to protect the homeland.

This week marks the first anniversary of the Department, and I would like to highlight for you some of the many accomplishments of IAIP.

Since March, 2003, IAIP has launched the Homeland Security Information Network, which is an interactive, collaborative, web-based system which reaches our customer bases more than ever before; and I am talking about State and local authorities and down to police chiefs and the rest within the first responder task forces of our country.

We have implemented the Homeland Security Presidential Directive 7, which addresses critical infrastructure, identification, prioritization and protection.

Through the National Cyber Security Division, we have established the U.S. Computer Emergency Readiness Team, or US–CERT, and launched the National Cyber Alert System only within the last few months, America's first coordinated cyber security system for identifying, analyzing, and prioritizing emerging vulnerabilities and threats. And I might add, as a sidebar, it is about making people aware of the situation regarding cyber threats to our Nation, both in the business side and the home user side as well.

We have assumed responsibility over this last year for the Homeland Security Operations Center, which is indeed the heartbeat in terms of information sharing and situational awareness for the Department.

We have formally executed the Protected Critical Infrastructure Information program, or the PCII, pursuant to the provisions of the Critical Infrastructure Information Act of 2002.

Now, even with these accomplishments, there is much work to be done, as many of you have highlighted in terms of your questions—and I include that so you understand I am on your frequency—staffing, categorizing our critical infrastructure and assets, ensuring private sector involvement in all that we do, particularly in terms of hardening critical infrastructure and putting protective measures in place, assuring the timely flow of threat information and protective measures to our customers across our great Nation.

To address these challenges, IAIP has instituted an aggressive hiring plan that will bring on approximately 40 new employees a month. We have worked with our partners at the State and local levels to refine our list of critical infrastructure, and we have 1,700 assets identified for action in 2004.

We are working with the private industry to help them not only understand their vulnerabilities but we are also providing recommended protective actions since, as was pointed out, they own about 85 percent and operate in support of 85 percent of the critical infrastructure of our Nation.

Through the Homeland Security Operations Center and the Homeland Security Information Network, we have increased our ability to share information with State and local officials in the private sector in an unprecedented fashion, real time collaborative effort, a two-way street that all resides operationally within our command center.

IAIP's budget relies on the expectation of two emerging trends, one, the nature and complexity of the threat, two, our national infrastructure components will become more complex and interdependent. These trends will result in more demands on the Department and on IAIP to anticipate terrorist intentions, tactics, capabilities and the responsibility to mitigate the risks and vulnerabilities and protect our country and our citizens.

For these reasons, the President's 2005 budget request for IAIP is structured around the following major programs: threat determination and assessment, $22 million; infrastructure vulnerability and risk assessment, $71 million; information and warning advisories, $60 million; remediation and protective actions, $346 million; outreach and partnership, $41 million; national communications system, $140 million; competitive analysis and

evaluation, $19 million; national plans and strategies, $3 million; and Homeland Security Operations Center, $35 million.

Let me discuss several initiatives associated with these mission areas for the 2005 budget request of $864 million.

This budget will allow IAIP to develop a detailed understanding of terrorist organizational capabilities with supporting materials and connectivity to interpret and predict threats.

Next, our budget funds the development of a comprehensive national infrastructure risk analysis and profile program.

Next, this funding supports submission of collection requests for threat information to the intelligence community and law enforcement establishments, disseminating guidance to homeland security components, developing analysis on the nature and scope of threats and identifying potential terrorist targets within the United States.

Another priority is the need to publish threat advisories, bulletins and warnings at a different level of classification to relevant stakeholders. Threat publications are detailed and disseminated in a timely fashion, portraying the nature, scope and targets of the threat.

The IAIP Directorate provides a broad range in services, including on-site planning advice, technical operational training programs, assistance in identifying vulnerabilities and developing and sharing best practices.

Activities in this area also include security efforts to protect infrastructure and key assets from cyber attacks. Specifically, the $345.738 million for remediation and protective action programs for critical infrastructure and key asset identification; critical infrastructure vulnerability field assessments; infrastructure and key asset protection programs; protection standards and performance metrics; and cyberspace security funding to ensure the continued healthy function of cyberspace.

The budget request allows the NCS to continue ensuring priority use of telecommunications services during times of national crisis, including the Government Emergency Telecommunications Service, or GETS. This funding also supports the development of the Wireless Priority Service, WPS, which provides a nationwide priority cellular service to key national security and emergency preparedness users, including individuals from Federal, State and local governments and the private sector.

Through the competitive analysis and evaluation program, we ensure that IAIP products and services are tested, that they are accurate and they are based on sound assumptions and data.

In summary, the 2005 budget request provide the resources to enable IAIP to manage and grow in its mission of securing the homeland. I come before you today to tell you that the progress that we have made has been solid; and there is absolutely no doubt in my mind that we, in terms of our efforts in support of defending the country, have made progress. While there is work to be done, we are safer today than we were a year ago, sir.

Sir, again, I am delighted to be before you, Mr. Chairman, and I am ready to take questions at this time, sir.

Mr. GIBBONS. Thank you very much, Under Secretary Libutti, for your very timely and helpful and constructive comments that you

have provided this committee. They will be very useful for us in our deliberations as well.

[The statement of General Libutti follows:]

PREPARED OPENING STATEMENT OF GENERAL FRANK LIBUTTI, UNDER SECRETARY FOR INFORMATION ANALYSIS AND INFRASTRUCTURE PROTECTION, DEPARTMENT OF HOMELAND SECURITY

Introduction

Good morning Chairman Gibbons, Representative McCarthy , Chairman Camp, Representative Sanchez and distinguished members of the Subcommittees. I am delighted to appear before you today to discuss the President's Fiscal Year 2005 budget request for the Department of Homeland Security's Information Analysis and Infrastructure Protection (IAIP) Directorate.

IAIP is the focal point for intelligence analysis, infrastructure protection operations, and information sharing within the Department of Homeland Security (DHS). Within a single directorate, IAIP merges the capability to identify and assess a broad range of intelligence and information concerning threats to the homeland, map that information against the nation's vulnerabilities, issue timely and actionable warnings, and take appropriate preventive and protective action to protect our infrastructures and key assets. IAIP is currently comprised of three primary components: the Office of Information Analysis (IA), the Office of Infrastructure Protection (IP), and the Homeland Security Operations Center (HSOC).

Fiscal Year 2004 Accomplishments

As we mark the first anniversary of the Department, I would like to highlight for you some of the many accomplishments of the IAIP Directorate, one of the newest parts of the federal government. The formation of IAIP has created for the first time a unique, integrated capability to not only map the current threat picture against the nation's vulnerabilities, but to also assess the risk of a terrorist attack based upon preventive and protective measures in place. That is, IAIP is enabling us to move from a reactive posture in the homeland to a risk management and mitigation posture. Let me give you some examples.

Since March, 2003, IAIP has:

- Launched the Homeland Security Information Network (HSIN), a comprehensive information sharing program that expands access to and use of the Joint Regional Information Exchange System (JRIES). The HSIN will provide secure real-time connectivity in a collaborative environment with states, urban areas, counties, tribal areas, and territories to collect and disseminate information between federal, state, local, and tribal agencies involved in combating terrorism.
- Coordinated Operation Liberty Shield and the rapid enhancement of security at more than 145 national asset sites at the outset of the war in Iraq. Following that, IAIP transitioned the protection of the sites from National Guard and law enforcement to a more cost effective and permanent set of physical protective measures.
- Enhanced protection, by assisting local communities with conducting vulnerability assessments and implementing protective measures, of the nation' highest risk chemical sites, thereby improving the safety of over 13 million Americans.
- Implemented Homeland Security Presidential Directive (HSPD) 7, "Critical Infrastructure Identification, Prioritization and Protection," which was signed by President Bush in December 2003. The HSPD assigned the Department of Homeland Security responsibility for coordinating the overall national effort to enhance the protection of the critical infrastructure and key resources of the United States and the development of an integrated cyber and physical protection plan.
- Implemented Wireless Priority Service, to ensure the continuity of cellular networks nationwide, registering over 3,000 federal, state, local and private users.
- Established the National Cyber Security Division (NCSD) to coordinate the implementation of the *National Strategy to Secure Cyberspace* and serve as the national focal point for the public and private sectors on cybersecurity issues, and developed a process for handling cyber incidents, successfully managing a number of major cyber events.
- Through the NCSD, established the U.S. Computer Emergency Readiness Team (US–CERT) through an initial partnership with the Computer Emergency Response Team Coordination Center at Carnegie Mellon University. US–CERT is building a cyber watch operation, launching a partnership program to build

situational awareness and cooperation, and coordinating with U.S. Government agencies to predict, prevent, and respond to cyber attacks.

• Launched the National Cyber Alert System under the auspices of US–CERT, America's first coordinated cyber security system for identifying, analyzing, and prioritizing emerging vulnerabilities and threats. This system provides the first nationwide infrastructure for relaying actionable computer security update and warning information to computer users in the government, in private industry, and small business and home users.

• Assumed responsibility for the Homeland Security Operations Center (HSOC), which maintains and shares real time domestic situational awareness; coordinates security operations; detects, prevents, and deters incidents; and facilitates response and recovery for all critical incidents and threats. As of February 2004, 26 federal and local law enforcement agencies and Intelligence Community members are were represented in the HSOC, providing reach back capability into their home organizations to continuously inform the current threat picture, and to provide key decision makers with real time information.

• Conducted detailed vulnerability studies of the banking and telecommunications industry to better understand the interdependencies and prioritize vulnerability reduction.

• Initiated an intra-Department and interagency review and analysis of information obtained in detainee briefings to assess specific terrorist capabilities, work that subsequently became the subject of several advisories disseminated to a variety of homeland security partners regarding terrorist planning, tactics and capabilities.

• Co-chaired with the Border and Transportation Security Directorate (BTS) the DHS Intelligence Activities Joint Study charged with reviewing the mission, responsibilities and resources of DHS Intelligence component organizations. The study was chartered for the purpose of making recommendations to the Secretary as to the optimal utilization of the Department's analytical resources.

• With the Homeland Security Council (HSC), initiated an ongoing interagency review of the Homeland Security Advisory System (HSAS), for the purpose of refining the system to make it more efficient and more beneficial for states and localities and the private sector.

• Formally executed the Protected Critical Infrastructure Information (PCII) implementing regulation, pursuant to the provisions of the *Critical Infrastructure Information ACT of 2002.* The purpose of the PCII Program is to encourage private entities and others with knowledge about our critical infrastructure to voluntarily submit confidential, proprietary, and business sensitive critical infrastructure information to the Department. Submitted information that qualifies for protection under the provisions of the Act and the PCII implementing regulation will be exempted from public disclosure, providing a significant opportunity for private entities to assist in homeland security without exposing potentially sensitive and proprietary information to the public. The Department will use information that qualifies for protection primarily to assess our vulnerabilities, secure the nation's critical infrastructure and protected systems, issue warnings and advisories, and assist in recovery.

Fiscal Year 2005

Even with these accomplishments, there is much more work that must be done. The United States remains at risk, despite the continuing work to assess and mitigate vulnerabilities. Our interdependent critical infrastructures enable Americans to enjoy one of the highest standards of living in the world, provide the backbone for the production of goods and services for the world's largest economy, provide over 60 million jobs, and ensure the United States can protect its national security interests. Infrastructure will remain one of the top priority targets for terrorists desiring to damage the nation?s economy and incite fear in the minds of the American people.

While the possibility of large-scale attacks similar to 9/11 remain significant, it is also possible likely that terrorists will employ smaller scale operations such as the suicide bombings prevalent in Israel. Terrorists understand that the cumulative effect of many small-scale operations—that are easier to plan and conduct ? can be just as effective as large-scale attacks in their overall impact on Americans? sense of security in their own country and, especially, at United States facilities overseas.

IAIP's budget relies on the expectation of two emerging trends: First, the nature and complexity of threats will increase; and, second, our national infrastructure components will become more complex and interdependent. These trends will result in more demands on the Department and IAIP to anticipate terrorist intentions, tac-

tics and capabilities, and to mitigate risks and vulnerabilities for the protection of the United States and its citizens.

For these reasons, the President's Fiscal Yyear 2005 budget request for IAIP is structured around the following major program areas: Threat Determination and Assessments, Infrastructure Vulnerabilities and Risk Assessments, Information Warnings and Advisories, Remediation and Protective Actions, Outreach and Partnerships, National Communications System, Competitive Analysis and Evaluations, National Plans and Strategies, and the Homeland Security Operations Center.

Threat Determination and Assessment ($21.943 Million)

IAIP's Threat Determination and Assessment program is designed to detect and identify threats of terrorism against the United States homeland; assess the nature and scope of these terrorist threats; and understand terrorist threats in light of actual and potential vulnerabilities within critical infrastructures and/or key assets. Addressing these issues requires the IAIP Directorate to improve on its existing set of threat analysts and analytical tools by hiring and training additional highly skilled threat analysts; acquiring and fielding new analytical tools and technologies to assist in assessing and integrating information; and deploying secure communications channels that allow for the rapid exchange of information and dissemination of analytical results.

These improvements will be used for multiple purposes, including: (1) providing analysis and assessments of the current threat picture as it relates to critical infrastructure; (2) developing actionable intelligence for Federal, state, and local law enforcement; (3) issuing warnings at all levels from the Federal Government to the private sector; and (4) supporting efforts to identify and coordinate effective countermeasures.

The President's Budget requests $21.943 million for continued support of on-going activities to continually form terrorist threat situational awareness, execute the functions outlined above, and focus on information sharing and coordination within DHS as well as in the Intelligence Community and other external stakeholder communities. These capabilities enhance the performance of two critical functions in protecting the homeland. First, it offers the United States Government the ability to integrate, synchronize, and correlate unique sources of information relating to homeland security, emanating from traditional and non-traditional (e.g., state and local governments, private industry) sources. Second, the IAIP Directorate is positioned to integrate knowledge of potential terrorist threats with an understanding of exploitable infrastructure vulnerabilities, resulting in a value-added profile of national risk that transcends traditional threat and vulnerability assessments.

Funding in this area is targeted to increase the IAIP Directorate?s technical competencies by training analysts and equipping IAIP with the most advanced technologies and tools. The training, tools and technologies will be utilized in four primary areas:

- **Model Terrorist Organization:** Developing a detailed understanding of terrorist organization capability with supporting materials and connectivity to interpret and predict threats.
- **Develop Terrorist Capabilities Baseline:** Developing a detailed understanding of terrorist capabilities baseline with supporting materials and connectivity to interpret and predict threats.
- **Collaboration and Fusion:** Expanding collaboration and fusion efforts from DHS to internal components, and out to an extended customer base.
- **Analysis Coordination:** Spearheading the effort to build a collaborative and mutually supporting analysis coordination schematic for DHS, and ensure that it incorporates others (TTIC, TSC, and the Intelligence Community) into a "community of interest" approach for understanding domestic terrorist threats.

Infrastructure Vulnerability and Risk Assessment ($71.080 million)

The Homeland Security Act directs the IAIP Directorate to carry out comprehensive assessments of the vulnerabilities of the critical infrastructure and key assets of the United States. As such, the IAIP Directorate serves as the focal point for coordination between the Federal government, critical infrastructure owners and operators, and state and local governments for the sharing of information and the planning for response to crisis events affecting infrastructures.

The Fiscal Year 2005 President's Budget requests $71.080 million to fund the development of a comprehensive National infrastructure risk analysis and profile (e.g., high value/high probability of success targets); development of analytic tools to evaluate critical infrastructure and key assets; and the coordination and development of a National threat vulnerability and asset database to access, integrate, correlate, and store threat and vulnerability information.

These mission areas will be enable IAIP to identify potential risks caused by infrastructure interdependencies, and determine the potential consequences of an infrastructure failure due to a terrorist attack. Ultimately, the intent of these efforts is to strengthen the capabilities of the IAIP Directorate and each critical infrastructure to provide near real-time notification of incidents; enhance the ability of the IAIP Directorate to assess the impact of incidents on critical infrastructure and key assets; to assess collateral damage to interdependent infrastructure; and create tools and processes to enhance infrastructure modeling and risk assessment capabilities.

The Fiscal Year 2005 budget request for infrastructure vulnerability and risk assessment is divided into three areas:

- **National Infrastructure Risk Analysis:** Funding in this area supports the development of comprehensive risk and vulnerability analyses on a national scale. These analyses are cross-sector in nature, focusing on problems affecting multiple infrastructures, both physical and cyber-related. As assigned in the Homeland Security Act and HSPD–7, the IAIP Directorate will continue to leverage and develop new techniques to map data provided by threat analyses, provide consequence analysis, and create vulnerability assessment teams based on the nature of the indicators or incidents. The goal is to produce timely, actionable information that is more meaningful to industry. A portion of this funding also supports the direct involvement of critical infrastructure sector experts to supplement risk analysis efforts and to gain a better understanding of the sector's core business and operational processes. In addition, a portion of this funding is utilized for exploration and to pilot innovative methodologies to examine infrastructure vulnerabilities and interdependencies.
- **Analytic Tools Development and Acquisition:** The IAIP Directorate will continue to collaborate with the Science and Technology (S&T) Directorate to acquire the most advanced tools and database designs available to better understand the complexities of interdependent systems and for translating vast amounts of diverse data into common and usable information for decision-makers, analysts, and infrastructure operators. Such capabilities include data-logging systems, modeling and simulation, data mining, and information correlation. Funding is targeted toward developing dynamic and multi-faceted tools designed to expand access to needed information.
- **National Threat/Vulnerability/Asset Databases:** The funding level requested for this activity in the fiscal year 2005 budget is based on the recognition of the data intensive nature, scale and complexity of analyzing infrastructure vulnerability issues. The intent is to develop and maintain databases that allow the IAIP Directorate to provide its stakeholders with up-to-date information on threats and vulnerabilities. Specifically, the IAIP Directorate is continuing to coordinate and direct the development of the primary database of the Nation's critical infrastructures through a collaborative process involving all stakeholders; maintain data on the risks posed to specific facilities and assets (and the probability of attack and associated consequences for homeland, national, and economic security should an attack occur); and develop, operate, and manage integrated data warehouses—in full compliance with the Department's privacy policies—that contain comprehensive all†source threat, vulnerability, and asset data.

Information and Warning Advisories ($59.807 Million)

One of the most visible aspects of the DHS mission lies in the management and administration of the Homeland Security Advisory System, the communications of threat condition status to the general public, and the continuous around-the-clock monitoring of potential terrorists threats. Specifically, there are three key information and warning activities that help support the Homeland Security Advisory System and other efforts to alert key Departmental leadership, national leaders and the general public: (1) tactical indications and warning and the associated warning advisory preparation and issuance; (2) information requirements management; and (3) integrated physical and cyber infrastructure monitoring and coordination.The Fiscal Year 2005 President's Budget requests $59.807 million to maintain the information and warning program. In addition to continuously operating a 24x7 capability, the information and warning program area will provide surge capabilities for the HSOC and with other Directorates during heightened states of alert or in response to specific incidents. The relevant fiscal year 2005 budget request is divided into three primary areas:

- **Tactical Indications and Warning Analysis/Warning Advisory Preparation and Issuance:** Funding in this area supports submission of collection requests for threat information to the Intelligence Community and law enforcement, disseminating guidance to DHS components, developing analyses on the

nature and scope of the threats, and identifying potential terrorist targets within the United States. A program priority is the continued to development of tools and technologies to assist our analysts to interpret, integrate, and catalogue indicators, warnings, and/or actual events and to provide Departmental and national leaders situational awareness. Another priority is the need to publish threat advisories, bulletins, and warnings at different levels of classification prior to distribution to the relevant stakeholders. Threat publications are detailed and disseminated in a timely fashion, portraying the nature, scope, and target of the threat. Ultimately, this information provides the basis for determinations to change the threat condition.

• Information Requirements Management: Information related to threats and critical infrastructure vulnerabilities are collected, stored, and protected within a diverse set of locations and sources, spanning all levels of government (Federal, state, and local) and including intelligence, proprietary and public sources. Funding in this area supports the technologies necessary to search within those diverse databases to identify, distill, and/or acquire mission-critical information. Program funding supports efforts to coordinate information requests and tasks emanating from within other parts of IAIP, other DHS Directorates, the Intelligence Community, law enforcement, state and local governments, and the private sector. In addition, a portion of these funds is used to supplement the information technology structure to accomplish these tasks efficiently and effectively through the use of leading-edge capabilities. This effort ensures that all information users are able to access all available and relevant data.

• **Integrated Physical and Cyber Infrastructure Monitoring and Coordination:** Intelligence and warning staff monitoring and coordination efforts ensure that threat and critical infrastructure issues are adequately addressed and represented. In addition, these efforts coordinate incident response, mitigation, restoration, and prioritization across critical sectors in conjunction with the other relevant DHS components (e.g., Emergency Preparedness and Response Directorate).

Remediation and Protective Actions ($345.738 Million)

The IAIP Directorate has established a national Critical Infrastructure Protection program that leverages stakeholder input at the Federal, state, and local level and across the private sector to provide the best and most cost-effective protective strategies for "at risk" infrastructure and facilities. Through this program, the IAIP Directorate provides a broad range of services including on-site planning advice, technical and operational training programs, assistance in identifying vulnerabilities, and development and sharing of best practices. Activities in this area also include security efforts to protect infrastructure and assets from cyber attacks (e.g., malicious software, distributed denial-of-service attacks).

1Specifically, the Fiscal Year 2005 President's Budget requests $345.738 million, for remediation and protective actions divided into the following five areas:

• **Critical Infrastructure and Key Asset Identification:** The Homeland Security Act directs the IAIP Directorate to recommend measures necessary to protect the critical infrastructure of the United States. One key step in this process is funding a national program focused on identifying critical infrastructure and assets and assessing potential risks of successful attacks to those assets. By understanding the full array of critical infrastructure facilities and assets, their interaction, and the interdependencies across infrastructure sectors, IAIP is able to forecast the national security, economic, and public safety implications of terrorist attacks and prioritize protection measures accordingly. Moreover, the process of identifying and prioritizing assets in this manner creates a common overarching set of metrics that consist of the individual attributes of specific infrastructure sectors.

• **Critical Infrastructure Vulnerability Field Assessments:** The Directorate coordinates with all relevant Federal, state and local efforts to identify system vulnerabilities and works closely with the private sector to ensure vulnerability field assessment methodologies are effective, easy to use, and consistently applied across sectors. Funding is targeted at the need to conduct and coordinate specialized vulnerability assessments by DHS teams, in conjunction with teams from other Federal or state agencies and private sector companies as appropriate, for the highest priority critical infrastructures and assets. The intent of these efforts is to catalogue specific vulnerabilities affecting the highest priority terrorist targets, thereby helping guide the development of protective measures to harden a specific facility or asset. A nationwide vulnerability field assessment program is currently underway leveraging the expertise of the IAIP Directorate, other agencies, and the private sector to ensure cross-sector

vulnerabilities are identified and that sound, informed decisions will be reached regarding protective measures and strategies.

• **Infrastructure and Key Asset Protection Implementation:** Due to the vast geographic size of the United States and diverse operating environment for each infrastructure sector, protection strategies must start at the local level and then be applied nationally as needed. Priorities for protection strategies are based on regional, state, and local needs and on the need for cross-sector coordination and protective actions within those geographic boundaries. The budget request reflects the need for the IAIP Directorate to continue the development of a flexible set of programs to assist in the implementation of protective measures. Examples include coordinating with other Federal and state agencies and the private sector to: (1) ensure the detection of weapons of mass destruction material is considered in the development of protection plans; (2) disrupt attack planning by taking low cost actions that make information collection and surveillance difficult for terrorists; (3) defend the most at risk critical infrastructure facilities and key assets throughout the country above the level of security associated with industry best practices; and (4) develop a nationally-integrated bombing response capability similar to that of the United Kingdom. DHS funding in these areas focuses on high value, high probability targets and will take the form of "joint ventures" with state and local governments, regional alliances, and the private sector.

• **Cyberspace Security:** Consistent with the Homeland Security Act and the *National Strategy to Secure Cyberspace,* a key element of infrastructure protection, both in the public and private sectors, is to ensure the continued healthy functioning of cyberspace, which includes the cyber infrastructure and the cyber dependencies in the critical infrastructure sectors. The IAIP Directorate recognizes that cyberspace provides a connecting linkage within and among many infrastructure sectors and the consequences of a cyber attack could cascade within and across multiple infrastructures. The result could be widespread disruption of essential services, damaging our national economy, and imperiling public safety and national security. The budget request supports efforts to capitalize on existing capabilities of the Directorate, and investing in new capabilities to monitor, predict, and prevent cyber attacks and to minimize the damage from and efficiently recover from attacks. As the manager responsible for a national cyber security program, the IAIP Directorate provides direct funding to support: (1) creating a national cyberspace security threat and vulnerability reduction program that includes a methodology for conducting national cyber threat and vulnerability risk assessments; (2) strengthening a national cyberspace security readiness system to include a public-private architecture for rapidly responding to and quickly disseminating information about national-level cyber incidents-including the Cyber Alert Warning System; (3) expanding and completing the warning and information network to support crisis management during cyber and physical events; (4) implementing a national cyberspace security awareness and training program; (5) developing capabilities to secure the United States Government in cyberspace that include guidelines for improving security requirements in government procurements; (6) strengthening the framework for national security international cyberspace security cooperation that focuses on strengthening international cyber security coordination and; (7) the Global Early Warning Information System, which monitors the worldwide health of the Internet through use of multiple data sources, tools, and knowledge management to provide early warning of cyber attacks.

• **Protection Standards and Performance Metrics:** Working in collaboration with the National Institute of Standards and Technology as appropriate, the IAIP Directorate is developing objective data for systems protection standards and performance measures. Several sectors currently use threat-based exercise approaches to validate key elements of their protection efforts. The budget request in this area will focus on continually improving and validating sector plans and protective programs and providing training and education programs for public and private sector owners and operators of critical infrastructure and/or key assets.

Outreach and Partnership ($40.829 Million)

The private sector and state and local government own and operate more than 85 percent of the Nation's critical infrastructures and key assets. Consequently, public-private cooperation is paramount, and without such partnerships, many of our Nation's infrastructures and assets could be more susceptible to terrorist attack. The IAIP Directorate is responsible for cultivating an environment conducive for public and private partnerships, developing strategic relationships underlying those

partnerships, and coordinating and supporting the development of partnerships between the Directorate and state and local government, private industry, and international communities for national planning, outreach and awareness, information sharing, and protective actions.

The Fiscal Year 2005 President's Budget requests $40.829 million to build and maintain a sound partnership foundation. It is imperative that the Department is familiar with the issues confronting the private sector, state and local governments, Federal sector specific agencies for critical infrastructure, and our international partners. Specifically, strong relationships must be maintained with the following communities of interest:

- **State and Local Governments:** Establishing and maintaining effective working relationships with State and local officials is a fundamental part of the DHS mission to effectively share information at unprecedented levels. IAIP is working with DHS' Office of State and Local Government Coordination to assess the information sharing and dissemination capabilities that exist nationwide in order to leverage existing capabilities and supplement capacity where needed.
- **Private Sector:** The Private Sector is another key partner in developing a nationwide planning, risk assessment, protective action, and information sharing strategy. Engaging the business community and making a business case for investment in protective and remedial strategies is key to our success.
- **Academia:** DHS will continue to develop, coordinate, and support partnerships with academic and other educational institutions. These partnerships will encourage and coordinate academic and other workforce development to assure availability of quality IT security professionals, and encourage curriculum development to integrate critical infrastructure protection (security) as normal elements of professional education.
- **Advisory Bodies:** DHS will also provide support to Presidential advisory bodies and cross-sector partnerships (including the National Infrastructure Advisory Council and the Partnership for Critical Infrastructure Security.)
- **International:** This funding will also support and enhance partnerships with the international community, working with and through DHS Office of International Affairs and the State Department, collaborating with the United States State Department on infrastructure protection activities. This includes bilateral discussions and activities on risk assessment and protective actions, information sharing, exercises and training. Of particular focus is the IAIP component of the Smart Borders implementation with Canada and Mexico. We will continue our role as the lead Federal Agency Role for the Information and Telecommunications Sectors. The Directorate will continue to partner with representatives from those industries composing the Information and Telecommunications sector and to educate members of the sector, develop effective practices, develop and implement intra-sector and cross-sector risk assessments, and work with other sectors on identifying and addressing risks associated with interdependencies.
- **Cyber:** We will expand the platform established by the Cyber Alert Warning System to include awareness and education programs for home users of computers and computer professionals in partnership with other Federal agencies and industry. Additionally, within private industry, our partnership and outreach efforts will involve the engagement of risk management and business educational groups to implement strategies to elevate senior management understanding of the importance of investment in cyber security.

National Communications System ($140.754 Million)

The national telecommunications infrastructure supports multiple mission-critical national security and emergency preparedness (NS/EP) communications for the Federal government, state and local governments, and the private industry. The security and availability of the telecommunications infrastructure is essential to ensuring a strong national, homeland, and economic security posture for the United States. The National Communications System (NCS) is assigned NS/EP telecommunications responsibilities through Executive Order 12472, *Assignment of National Security and Emergency Telecommunications Functions,* which include: administering the National Coordinating Center for Telecommunications to facilitate the initiation, coordination, restoration, and reconstitution of NS/EP telecommunications services or facilities under all crises and emergencies; developing and ensuring the implementation of plans and programs that support the viability of telecommunications infrastructure hardness, redundancy, mobility, connectivity, and security; and serving as the focal point for joint industry-government and interagency NS/EP telecommunications planning and partnerships.

The Fiscal Year 2005 President's Budget requests $140.754 million for the capabilities and analytic tools necessary to support the expansion of NS/EP telecommunications programs and activities. The fiscal year 2005 funding level ensures a continuation of the NCS mission and legacy NS/EP telecommunications programs and assets. Specifically, the fiscal year 2005 budget request for the NCS is divided into four areas:

- **Industry-Government and Interagency Processes:** The NCS has cultivated and expanded its relationships with the telecommunications industry and other Federal agencies to promote joint planning, operational activities, coordination, and information sharing. The primary industry partnership is the President's National Security Telecommunications Advisory Committee (NSTAC), which is comprised of 30 industry leaders representing various elements of the telecommunications industry. The NSTAC and its subordinate body, the Industry Executive Subcommittee (IES), provides industry-based analyses and perspectives on a wide range of NS/EP telecommunications issues and provides policy recommendations to the President for mitigating vulnerabilities in the national telecommunications infrastructure. Paralleling this industry relationship is the interagency process involving the NCS Committee of Principals and its subordinate body, the Council on Representatives, which facilitate the NS/EP telecommunications activities of the 23 Federal agencies constituting the NCS.
- **Critical Infrastructure Protection Programs:** Leveraging the industry relationships described above, the NCS manages several network security and CIP-related programs, including: (1) the National Communications Center (NCC), a joint industry—and Government-staffed organization collocated within the NCS and serves as the operational focal point for the coordination, restoration, and reconstitution of NS/EP telecommunications services and facilities; (2) the Telecommunications Information Sharing and Analysis Center, which is the focal point for the generation, compilation, and sharing of cyber warning information among the telecommunications industry; (3) the Government and National Security Telecommunications Advisory Committee Network Security Information Exchanges (NSIEs), which meet regularly and share information on the threats to, vulnerabilities of, and incidents affecting the systems comprising the public network; (4) the Critical Infrastructure Warning Information Network (CWIN), which is designed to facilitate the dissemination of information and warnings in the event of a cyber attack; (5) Training and Exercises, which helps ensure the readiness and availability of qualified staff to perform the operational duties of the NCS associated with Emergency Support Function #2—Telecommunications of the Federal Response Plan; (6) Operational Analysis, which develops and implements tools and capabilities to conduct analyses and assessments of the national telecommunications infrastructure and its impact on NS/EP services; (7) NCS also supports the Global Early Warning Information System, which monitors the worldwide Internet health through use of multiple data sources, tools, and knowledge management to provide early warning of cyber attacks, (8) Shared Resources (SHARES) High Frequency (HF) Radio Program, developed by the NCS and in continuous operation since being approved by the Executive Office of the President in the NCS Directive 3–3 of January 1989. The SHARES program makes use of the combined resources and capabilities of existing Federal and federally affiliated HF radio stations on a shared, interoperable basis to provide critical backup communications during emergencies to support national security and emergency preparedness (NS/EP) requirements.
- **Priority Telecommunications Programs:** The NCS is continuing a diverse set of mature and evolving programs designed to ensure priority use of telecommunications services by NS/EP users during times of national crisis. The more mature services—including the Government Emergency Telecommunications Service (GETS) and the Telecommunications Service Priority (TSP)—were instrumental in the response to the September 11th attacks. Fiscal Year 2005 funding enhances these programs and supports the development of the Wireless Priority Service (WPS) program and upgrade to the Special Routing Arrangement Service (SRAS). Specifically, priority service programs include: (1) GETS, which offers nationwide priority voice and low-speed data service during an emergency or crisis situation; (2) WPS, which provides a nationwide priority cellular service to key NS/EP users, including individuals from Federal, state and local governments and the private sector; (3) TSP, which provides the administrative and operational framework for priority provisioning and restoration of critical NS/EP telecommunications services; (4) SRAS, which is a variant of GETS to support the Continuity of Government (COG) program including the

reengineering of SRAS in the AT & T network and development of SRAS capabilities in the MCI and Sprint networks, and; (5) the Alerting and Coordination Network (ACN) which is an NCS program that provides dedicated communications between selected critical government and telecommunications industry operations centers.

• **Programs to Study and Enhance Telecommunications Infrastructure Resiliency:** The NCS administers and funds a number of programs focusing on telecommunications network resiliency, security, performance, and vulnerabilities, including: (1) the Network Design and Analysis Center, which is a set of tools, data sets, and methodologies comprising the Nation's leading commercial communications network modeling and analysis capability that allows the NCS to analyze the national telecommunications and Internet infrastructures; (2) the NS/EP Standards program, which works closely with the telecommunications industry to incorporate NS/EP requirements in commercial standards and participates in national and international telecommunications standards bodies; (3) the Converged Networks Program, which investigates vulnerabilities and mitigation approaches in future technologies and networks (specifically Internet Protocol-based networks); (4) the Technology and Assessment Laboratory, which provides the ability to evaluate penetration testing software, modeling tools, various operating systems and protocols, hardware configurations, and network vulnerabilities, and; (5) the Routing Diversity effort, which is developing a communications routing diversity methodology to analyze a facility's level of routing diversity and is evaluating alternative technologies which can provide route diversity, and (6) the NCS, through various associations and other activities is involved in a variety of International Activities (NATO, CCPC, CEPTAC, and Hotline) which provides technical subject matter expertise, guidance, and coordination on CIP issues affecting the telecommunications infrastructure in numerous international forums on behalf of the United States Government.

Competitive Analysis and Evaluation ($18.868 Million)

The Competitive Analysis and Evaluation program ensures that IAIP products and services are tested, accurate, based on sound assumptions and data, and ultimately, offer the highest quality, depth, and value to IAIP customers. The Fiscal Year 2005 President's Budget requests $18.868 million to provide for the unbiased, objective analyses and evaluation of IAIP findings, assessments, and judgments through three functional areas: Risk Assessment Validation, Evaluation, and Exercises and Methodologies.

• **Risk Assessment Validation:** Funding is used to establish and field physical and cyber target risk analysis teams that employ "red team" techniques to evaluate measures taken by other IAIP components to protect key assets and critical infrastructure. The red teams emulate terrorist doctrine, mindsets, and priorities and employ non-conventional strategies to test and evaluate IAIP planning assumptions.

• **Evaluation:** Funding supports several initiatives, including the IAIP Product and Process Evaluation, which involves conducting independent, objective evaluations of IAIP products and processes and to assist IAIP divisions to develop products that offer value to IAIP customers. The second is IAIP Customer Satisfaction, which evaluates customer satisfaction with IAIP products and services to ensure they are responsive to current customer needs. Funding in this area provides for electronic and non-electronic feedback surveys, field visits, and conferences.

• **Exercises and Methodologies:** Coordinate and manage interagency exercises and tabletops that test both DHS and IAIP policies, processes, procedures, capabilities, and areas of responsibilities. Participating in and conducting after action reviews of exercises provides invaluable experience and feedback related to capabilities, connectivity, and information sharing during a crisis event. Investment in this area informs the Department's decision as to where improvements are needed. This funding also supports examining and instituting advanced methodologies such as alternate hypotheses, gaming, modeling, simulation, scenarios, and competitive analyses to ensure IAIP products are accurate, sophisticated, and of the highest quality and value to customers.

National Plans and Strategies ($3.493 Million)

Critical to ongoing national efforts to protect and secure the homeland are updating, revisiting, coordinating the development, and monitoring the implementation of National Plans and Strategies. The Fiscal Year 2005 President's Budget requests $3.493 million to support activities by coordinating, developing, and publishing contingency planning documents for critical infrastructures (as called for in the *Na-*

tional Strategy to Secure Cyberspace), monitoring progress against those documents, and producing an annual report.

Homeland Security Operations Center ($35.0 Million)

The HSOC maintains and shares domestic situational awareness; coordinates security operations; detects, prevents, and deters incidents; and facilitates the response and recovery for all critical incidents. The HSOC is the focal point for sharing information across all levels of government and the private sector.

The HSOC facilitates the flow of all-source information and develops products and services including: (1) the daily Homeland Security Situation Brief for the President, (2) reports and briefs to law enforcement, the Intelligence Community, other Federal and state agencies and industry partners, (3) warnings and alerts to individual responder agencies and the public as appropriate, and (4) coordinated response when crises do occur. The HSOC concept is to draw from the many distributed systems and centers that are currently dedicated to different missions and optimize their contribution to homeland security.

HSOC funding will help with the time efficiency of issuance of information and warning advisories through increased operations efficiency brought about by facility improvements.

New Programs

In the fiscal year 2005 IAIP budget, as a part of an interagency effort to improve the Federal Government's capability to rapidly identify and characterize a potential bioterrorist attack, the President request $11 million for a new biosurveillance iniative. This increase provides for real-time integration of biosurveillance data harvested through the Centers for Disease Control (CDC), Food and Drug Administration (FDA), United States Department of Agriculture (USDA) and DHS Science and Technology (S & T) Directorate with terrorist threat information analyzed at IAIP. Currently, a finding from one source of surveillance exists in isolation from relevant surveillance from other sectors, making it difficult to verify the significance of that finding or to recommend appropriate steps for response. Integrating the information in IAIP, and analyzing it against the current threat picture will inform effective homeland security decision-making and speed response time to events.

This interagency initiative, includes DHS's ongoing BIOWATCH environmental biodetection program, Health and Human Services' (HHS) proposed BIOSENSE program, HHS' and United States Department of Agriculture's (USDA) ongoing joint separate food security surveillance efforts, and USDA's agricultural surveillance efforts. This DHS-led effort will promote data sharing and joint analysis among these sectors at the local, state, and Federal levels and also will establish a comprehensive Federal-level multi-agency integration capability to rapidly compile these streams of data and preliminary analyses and integrate and analyze them with threat information

Conclusion:

In summary, the fiscal year 2005 budget request provides the resources to enable the IAIP Directorate to manage and grow in its mission of securing the homeland. I look forward to working with you to accomplish the goals of this department and the IAIP directorate.

Mr. Chairman and Members of the Subcommittees, this concludes my prepared statement. I would be happy to answer any questions you may have at this time.

Mr. GIBBONS. We will turn to members for 5 minutes or for those people that did not make an opening statement an additional 3 minutes to their time to ask questions.

I will begin by asking you a sort of "current events" topic today. The Congressional Quarterly this morning is reporting that the Heritage Foundation is about to release a report that is somewhat critical of the Department for being—and I will quote their statemen—just another end user, end quote, of intelligence information.

The article further implies that the Department of Homeland Security is not a full partner, because it does not have oversight authority over TTIC.

Could you address this issue for the committee? Is DHS a full partner at TTIC, or is DHS simply just another end user of the information?

General LIBUTTI. I appreciate the questions, sir. It gives me a chance to share with you my views relative to not only TTIC but our charge and responsibility.

As you all know, we are the newest member of the Federal intelligence community, and we full members. We are not red-shirting. We are not standing in the back of the bus. We are full players. We demand excellence. We interact with members of the community across the country in terms of providing input to us from State and local, private sector.

In terms of the TTIC response, I would tell you this. We are part of the TTIC. We are TTIC. The key players in TTIC are the CIA, the FBI and Homeland Security. Members of Homeland Security work in the spaces and operation and function within the TTIC environment.

TTIC's key point in terms of function is integration. They bring together foreign and overseas data and intelligence. They combine that with input from Homeland Security, the Justice Department, key point, FBI, and they integrate, fuse, analyze and share it with their customer base, which are the key players in the Federal Government.

When we receive that information, we are charged to and absolutely every day execute comparative and competitive analysis of that information. And what is different about what we do, sir—and ladies and gentlemen—is that we focus on the domestic scene, and we do so, again, in concert with our customer base.

So when we analyze information relative to a threat, be it general or specific, we take that input which our folks at TTIC have helped in supporting development of, and we provide to our IA leadership, General Pat Hughes, input from State and local folks. We analyze that with a view towards action, protective or preventive action, in support of protecting the country.

Quite frankly, I see TTIC as a great effort, a great initiative set up, established at the right time, at the right place, as the country looked for a service to function and integrate intelligence. For me and from my standpoint, it is working.

I just glanced very quickly this morning at the Heritage article. I respect the leadership at Heritage. They have not called me or talked to me about their concerns or their viewpoints. I dare say, although I don't know this for fact, they probably didn't talk to General Pat Hughes either or any of our folks in our intelligence organization. But I dare say perhaps with further investigation that investigation would reveal that, number one, we have a principal, primary mission to support and protect the homeland. We are in the intelligence business. Our focus is different than the agency, the CIA, or TTIC, and I think we are doing it smartly.

Mr. GIBBONS. Mr. Secretary, I gather from your comments that you feel the article was either inaccurate or misrepresentative of the facts?

General LIBUTTI. Sir, again, I glanced at it very briefly. I would say that if indeed the article represents a notion that we are not full players, that is absolutely incorrect.

Mr. GIBBONS. Let me ask a very brief question. I have 40 seconds to do this, and hopefully we can get through it.

There have been a lot of news articles and reviews recently reporting that the terrorist watch list is not functional and that border security officials and law enforcement personnel don't have easy access to this information. I think we all understand that the Terrorist Screening Center is an FBI program. Could you briefly address this issue from the perspective of a customer of the Terrorist Screening Center?

General LIBUTTI. The FBI Department of Justice does lead the effort now. I think it is a feather in the cap of the Department of Justice and overall those who deal with countering terrorism in the country that the Terrorist Screening Center is alive and well, up and functioning and producing great results.

The bottom line in terms of what that center is about is to help the cops on the beat at State locations, providing a single point of contact for entry into the national system which would ask appropriate questions regarding those we suspect of being terrorists or conducting terrorist activity. It is still in its initial phases.

As you all well know—and if you don't I will provide a quick summary—one, the charge is work day-to-day now; and they are doing that. I would tell you that my recollection is that there have been since 1 March 1,388 inquiries into that system and 527 positive hits that have helped law enforcement across the country deal with the situation at hand. I mean, that has got to mean something in terms of not only the operational side of it but what we see as a way ahead in terms of what we expect in the future when the program is fully mature.

My recollection as well is that local cops have access to over 50,000 records that are now part of what is available to cops on the beat.

My recollection as well is that we had hoped to complete the second aspect of the Terrorist Screening Center and the Department of Justice and the FBI's work is that we would take numerous watch lists and integrate them into a single database. That effort, indeed, may take longer than we had expected as an effort we could do by this summer.

But the point of fact is the system is working. The clarification, purification, adjustments of the watch list is being done, and a single database is indeed being developed.

So the system works now; and, as I said earlier, I think it has had tremendous credibility in terms of how cops see that system working now to support them.

Mr. GIBBONS. Thank you very much.

I will turn now to Ms. Sanchez of California for 5 minutes.

Ms. SANCHEZ. Thank you, Mr. Chairman.

Well, I asked a whole bunch of questions in the beginning, so let me just go over a couple of them, and maybe you can get to them quickly.

The first one was on the critical infrastructure and having the database listing. As I said, Mr. Liscouski had said that it would be completed within 5—might be completed within 5 years. What is the right estimate? Who is in charge of the effort? What methods are being used to prioritize that critical infrastructure? How comprehensive is the database going to be? I know that this is an un-

classified setting, but can you tell us generally what is included, what industries, what public infrastructure?

Secondly, if you could speak, please, to the funding decrease for the risk assessment in fiscal year 2005. If we don't have a completed assessment yet and we are not going to have it for 5 years, then why are we cutting the funding in that category? Aren't you concerned that we are not getting adequate staff to do this or adequate funding to do it, considering it has been 2 years—over 2 years since 9/11 and this committee has seen nothing done with respect to this work yet?

General LIBUTTI. Well, I respect your comments, ma'am, but I must say there has been an awful lot done in terms of risk assessment, contacts that we have made in IAIP with Bob Liscouski in the lead and his magnificent team. We plan on moving forward over the next year to look at 1,700 facilities. When you lay that out against the thousands of infrastructure facilities across the country, you would say, well, that may not be much more than a drop in the bucket, except with this footnote.

What we have done with the private sector and business leaders is looked across the country at what we believe are key, critical infrastructure sites or facilities, and we have prioritized our efforts to deal with those facilities that we think are what I call critical centers of gravity, the loss of which would result in economic failure, lack of trust from the American people and a catastrophic failure in terms of function of the cities and areas around those facilities.

So that has been done. We have connected with people in the private sector as well as State and local authorities.

Ms. SANCHEZ. So this security that is being done on these very critical situations that you have said you have already taken a look at, has there been Federal money spent to help fortify that or not?

General LIBUTTI. Money out of my Directorate has been spent, was spent in 2003 and is now being spent to support, one, identifying that which is most critical, two, working to analyze the actions that need to be taken—we call protective measures—to reinforce or harden those facilities or targets and—.

Ms. SANCHEZ. Why is that information not shared with the Subcommittee on Critical Infrastructure?

General LIBUTTI. I can't answer that, ma'am. I am surprised to hear you say that. I will make every effort and—.

Ms. SANCHEZ. I mean, we have asked over and over for some sort of list or what are you doing or what is the infrastructure you are protecting or what should we protect. Because remember, after all, we are the ones that control the dollars to all of this.

General LIBUTTI. Ma'am, you are absolutely right; and I hear you loud and clear. Let me outline within this 1,700 number I gave you where we are going.

Ms. SANCHEZ. And how did you choose the 1,700? I mean, this is the question we all have. We don't know.

General LIBUTTI. I will do my very best to answer your question, ma'am.

The broad areas that we are looking at with a priority of effort, the chem sites, nuclear power plants, soft targets, for example, shopping malls, stadiums and the rest, electric power substations

and mass transit systems—when people ask me, Frank Libutti, what are your concerns overall in terms of how you see the threat and that which will be paramount in your mind in terms of protective action working with the private sector and the other folks in the intelligence community and our other customer base, I would tell you, broadly speaking, it is transportation, it is aviation—transportation at large, aviation and energy.

The points I just made relative to where our current focus is represents the priority of action in terms of where we are going to go over the next year, and I regret that you are not informed relative to that. I will make a very special effort to—.

Ms. SANCHEZ. Great. So I can get a list of the 1,700

General LIBUTTI. To bring those details to you, ma'am.

Ms. SANCHEZ. Whether it has to be in a secret meeting or what have you. But, I mean, we really have been asking for this information, and we have seen nothing.

General LIBUTTI. You asked how we arrive at this. In our business, in terms of how Intel informs actions, other than the Intel actions which we refer to, setting requirements, collecting against requirements, analyzing that and taking actions, that is the Intel side. But the real action side of what we do, something that should be and will be measured and shared with you all, is Bob Liscouski's action. My expectation is not only will we hold meetings, conference calls and councils across the country with appropriate ISACs and CEOs, I am looking for material changes that really make a difference in terms of the physical plant. And we are working towards that. That is a priority for what we are all about.

Again, I will be happy to share that with you or ask Bob Liscouski to share that with you as well.

Ms. SANCHEZ. Thank you, Mr. Chairman. I see that my time has expired. Thank you.

Mr. GIBBONS. Thank you, Ms. Sanchez.

We will return now to the chairman of the full committee, Mr. Cox, for 5 minutes.

Mr. COX. Thank you, Mr. Chairman.

Welcome, Mr. Secretary. I want to cover just one or two topics, but I have a lot of little, detailed questions. So I am going to do something unusual and ask you to just jot down some notes. I am going to start out with eight little questions about factoids that I think you can just tell me you know the answer to or you don't and you can get back to us, if that is all right.

The first—and the two topics concern, first, IAIP growth plans and how you are staffing up; and the second concerns the downstream role of TTIC and the relationship of TTIC to IAIP.

So here are eight questions that I hope will elicit some data in response.

First, your budget request this year, the Department's budget request, seeks to fund 19 new analysts in IAIP, and I am just wondering what that represents in terms of a percentage increase, how many you have currently.

Second, where are we getting these 19 people? Are these going to be fresh hires from universities, or will we fish in some other pond?

Third, how long will it take to bring the 19 up to full capability?

Fourth, are they going to be hired for specific subject matter expertise, for example, in biohazards?

Fifth, inasmuch as there are other intelligence agencies that are also hiring analysts and some of them have more established brand names, does Congress need to help you provide additional incentives so that you can attract the kind of analysts that you need? Are you thinking about that, or do you need to—.

General LIBUTTI. I can answer that question, if I may interrupt and say as I said earlier—and I don't mean this to be—try to be cute. We need all the help we can get, and I will talk when you finish, sir, about our way ahead in terms of staffing, planning, recruiting efforts, et cetera. But certainly any encouragement, particularly from a gentleman of your persuasion and reputation, is going to make a difference, and I thank you for it.

Mr. COX. Well, to try and throw that question more in the category of the others so that you can respond with just—that could be a difficult conceptual topic to get into, but, you know, very specifically, do you need authority for more money in order to do that?

Six, does DHS and do you at IAIP have your own training program for your analysts? How will they be trained? By whom? Is there a set program, for example.

Seventh, what is the current percentage of your analysts at IAIP who are detailed from other Federal agencies?

And eighth, and finally, what percentage of IAIP's analysts are now contractors or annuitants?

You may be able to answer some or all of those with the information you brought, and possibly you will have to get back to us. I would appreciate that either way.

The other question relates to TTIC. I have a transcript of an interview on Fox News, or at least a news story on Fox News, quoting John Brennan at TTIC. Mr. Brennan repeats something we have heard in this committee before, that Homeland's mission stops at the U.S. shore. It concerns me a great deal, because I think it is abundantly clear that the mission does not stop at the U.S. shore. There is absolutely nothing in the Homeland Security Act that suggests that.

As a matter of fact, today's terrorist threat to the people who live in America's cities and towns is an overseas-directed threat, and the information that we are eliciting from questioning of Al- Qa'eda operatives in Guantanamo is leading us not only to the place that they might conduct their activities in the United States but also to their overseas bases and to the organizations that are both directing these things and recruiting additional people to do it. We set up the Homeland Security Department so that we would have someplace where we could deal with this unique threat with the nature of this.

What I will say is TTIC's unique disadvantage is just the opposite of what Mr. Brennan is saying, and that is that TTIC, under the direction of the DCI and de facto if not de jure under the control of the CIA, cannot, should not and must not be involved in domestic U.S. homeland security.

Mr. COX. They are essentially an overseas operation, so we have to have TTIC and IAIP to perform those statutory functions.

I just want to leave you with section 201(D) of the act which I am fond of quoting. It is, in fact, the law, and it says that first on a list of your responsibilities is to access, receive, and analyze law enforcement information, intelligence information, and other information from agencies of the Federal Government, State and local government agencies, including law enforcement agencies and private sector entities, and to integrate such information in order to identify and assess the nature and scope of terrorist threats to the homeland, detect and identify threats of terrorism against the United States, and understand such threats in light of actual and potential vulnerabilities of the homeland.

I cannot for the life of me see how that mission differs from TTIC's. I think they have set themselves up as a direct competitor.

So my second question to you is, can we anticipate down the road a plan for Homeland to acquire control over this operation, which the Inspector General says is a competitor that is diminishing your opportunity to do your job?

And I want to conclude all of these questions by saying, I ask these in a spirit of complete, unequivocal support for your mission and what you are doing. This committee is the strongest booster for the Department in Washington that you are going to find. We want you to be as effective as possible in fulfilling those statutory mandates. That is a lot, but—.

General LIBUTTI. Sir, I will do my very best with the time constraints and the rest, and mind my manners in that regard. So I will try to get through key points. One is the manpower piece, TTIC, and related questions, that which I do not have a chance to answer, so we will provide that back to you and to the chairman as requested.

General LIBUTTI. But let me start with the last point. Again, I was the Commissioner For Counterterrorism in New York City when all of this came about in terms of the establishment of TTIC. So when I came in as prepped for my hearings, I had to get smart on TTIC, the interaction with IAIP, the Department of Homeland Security, and other members of the Intelligence Community. And at the time, and as I now feel, the establishment and stand-up of TTIC was the right thing at the right time under the right leadership. Our relationship with John Brennan as the leader of that organization has been superb.

As I said or alluded to, and I will try to restate it more clearly now when I reference the point that we are TTIC, I believe that in my heart, I believe that intellectually. We are both customer and contributor to the TTIC effort, and I think it has been more than satisfactory in terms of supporting our needs as an integrator and an organization that is not per se operational, nor does it per se collect, but it gathers. We are in the business of taking that information and intelligence and actioning it to people that have a responsibility to protect the homeland, both in the Federal Government and in the State and local arenas. There is my bottom line in terms of your last point. In the future, we ought to be open enough to keep all options on the table relative to any organization that supports the intelligence effort of this great country.

Let me move to manpower, sir, and you know most of this, so I will try to cut through the details and provide bottom line execu-

tive ceremony. When IAIP inherited positions from five legacy organizations, the vast majority of which were vacant; that is, we got the authority but people did not come with that, and the numbers I want to share with you are 409 vacant of 544 total for 2003. We put into place an aggressive hiring plan. That plan includes the following: identification of our unique needs. We are talking people that have to, at the end of the day, to fully support our operation, have Top Secret/SCI clearances, because the space I work in is a SCIF space.

Next, we have been using contract support to help us write position descriptions, advertise the jobs, conduct interviews with appropriate candidates, and alluding to one point you made earlier, I would just say in a broad sense we are looking for at every corner to recruit, in academia, young, hard charges coming out of the service, people who have been long-standing experts in the intelligence field. There are no holds barred, no restrictions in terms of those we are looking at to bring into this and bring onto this great team.

The plan is to bring 40 new employees a month on board. We currently have on board 263 full-time employees, with another 100 positions in the hiring process. What that means is we have interviewed 100 people, and I am hoping and praying, saying my rosary, that the majority of those folks are motivated to come on board and support us, because we need them, and you are absolutely right.

These folks are supplemented by 214 detailees and contractors for an on-board strength of 471 people. Please understand, as I know you do, sir, but permit me to carry on, it is a heck of a challenge in trying to find qualified folks, because the competition in this town is not simply in terms of the Federal Government, including intelligence agencies, but it is with the private sector, the private sector who is appropriately reaching out and doing business with us in the area of homeland security, and IAIP needs the same credentials and classification requirements as my folks need.

So back to a point you made earlier, and it is not about money, because we got enough money; it is about the reputation and encouragement of everybody in a leadership position in this town to help us recruit. And I would ask you to help me with that, sir.

One of the challenges we have, and my staff and I are focused on this big time, I think it gets back to a question that Representative Turner raised, or maybe even just suggested we look at, and we are, sir, and that is the whole classification system. It takes a year or a year-and-a-half to get somebody cleared and, quite frankly, being the infantry guy I am, a fairly simple person in terms of getting things done, I want to get things done. And while I am not criticizing the current system, because it is appropriate given the guidelines that we all work under now, I am going to try to move forward and ask folks to deal with that, to look hard at the whole classification system. Not that we would circumvent the requirement to bring in people that are clean as a whistle, that have great integrity and can deal with classified material, but the fact is it slows the heck out of what we are trying to do.

The question relative to analysts in IAIP, we have 74 FTEs and 37 detailees for a total of 111 people. And given my approach towards recruiting, we can bring on 40 or so a month, and we will

move ahead to close the gap and meet our objectives in terms of hiring.

Sir, that just touches broadly on your two questions. I am happy again to provide answers on the following additional questions you rifled at me in terms of experts to deal with biohazard and the training piece and the rest, and I am happy to do that, with your blessing.

Mr. COX. As follow up, that is fine.

General LIBUTTI. Yes, sir. Appreciate it, sir.

Mr. GIBBONS. Thank you very much, Mr. Cox. We will turn now to Ms. McCarthy for 5 minutes.

Ms. MCCARTHY. Thank you, Mr. Chairman. And thank you, sir, for your testimony here today.

I want to follow up with you, first of all, by telling you how pleased I am that you are requesting an increase in funding for communication skills and efficiency of informations and warnings, and I thank you for sharing the good news with us about the watch list improvements for our police. You have been on the frontline in New York and in the world of the police department, and so you know how vital that is.

You mentioned in your testimony that there is going to be improvement on the wireless service for Federal, State, and local officials, and that is truly one of the key topics I hear from my first responders when I am talking to them in the district.

Would you explain a little bit more about that wireless service that you mentioned and how it is going to be interoperable? I hope that is under consideration; I did not hear that in your remarks, and I wonder if it does include interoperability, because I think that that is one of the most important things our first responders bring up with us. They need timely, usable information from the Department, and then they have to make informed decisions and hopefully prevent some sort of terrorist incident out there in America, and there are, of course, several methods and ways to share information. But I wonder what type of information IAIP plans to share with State and local officials and the methods that they will use to pass this along, particularly in a timely way.

General LIBUTTI. I thank you for the question. It reflects our priority as well. I know that you all are aware of the initiative the Secretary rolled out last week in Washington and I rolled out in St. Louis last week. It is called our Homeland Security Information Network. I am on my way to Florida and other places across the country to initiate that program and improve what I would call our ability to communicate and share information.

To the point that you asked, ma'am, regarding interoperability, that is a concern of ours, but the lead agency for that piece of communications, info-sharing, is science and technology. But I will turn my attention now to attempt to address your questions regarding wireless. But when you mention that word, interoperability, what is to me is I am a user of technology, and the technology wizards are in S & T and not in my shop.

But I do want to just briefly talks about GETS, which I mentioned earlier, which is about the land side, and the WPS, what is the cellular side. I just want to cover key points that I put together

in my notes, appreciating the fact that you would have questions on this.

The goal of the Wireless Priority Service, or what we call WPS, is to enhance the Nation's cellular telephone infrastructure with priority capability that gives national security and the emergency preparedness community priority communications at all times under all circumstances. The WPS is designed to provide critical users a high probability of call completion during periods of extreme communication network congestion; for example, during 9/11, major hurricanes, storms, or, God forbid, another terrorist attack.

The wireless infrastructure in the United States consists primarily of two technologies offered mainly by the six major nationwide carriers and almost equally deployed. The global system for mobile communications, GSM, for AT & T Wireless, Cingular Wireless, Nextel and T-Mobile, and Code Division Multiple Access, we call CDMA, for Verizon Wireless and Sprint PCS, just to give you a sense of what we are after in terms of land and cell, and then who is doing that and who we expect to complete those actions.

Ms. MCCARTHY. Mr. Secretary, I appreciate that knowledge, and I would be happy for you to just get that to me to read thoughtfully and also have available for my conversations with my first responders at home.

General LIBUTTI. Yes, ma'am.

Ms. MCCARTHY. Speak to me about how confident you are about achieving this and when, because you are right, when you mentioned storms, during a severe ice storm a couple of years ago in my community, my fire and police could not talk to each other. They wanted to help out, they ended up using their cell phones.

General LIBUTTI. Yes, ma'am. Again, my New York experience brings me to that same conclusion. At State and local levels that needs to be improved and improved with a real strong energy, strong vector at let's make it work.

Back to a point I made earlier. The S & T folks are looking across the country at all technologies off the shelf, what the future looks like, and they are the ones that are providing the technology advanced concepts in support of folks in the cities and States. My job, again in support of science and technology, is to be a good listener in terms of what first responders are saying and to hold that up against the threat. So technology and supported communications interoperability must make sense in terms of what we know about the tactics, techniques, and operational capabilities of the bad guys. So that is my role in that.

Ms. MCCARTHY. I appreciate that role.

General LIBUTTI. I want to just cover something, if I may.

Ms. MCCARTHY. Let me just suggest something to you, sir, out of respect to time and the other concerns of the committee.

I appreciate that you are a good listener; I know you are. I would like you to be a big bell ringer. I would like this to become a priority, not just in the science and technology end, but in your end as well, because really, truly, that is the number one issue I hear over and over again from the first responders, is the need for that. And I believe we need to make it a priority, and I would like your involvement in that goal.

General LIBUTTI. Yes, ma'am. I do want to cover if I may, Mr. Chairman, just continue very quickly, and again it is just stats that I put together to share with you.

In terms of the GETS program, currently there are approximately 82,000 users of that program. In the wireless program that we refer to, the priority service currently, 3,000 users and rapidly growing operational in terms of the T-Mobile network, AT & T Wireless, and Cingular, we expect to come up this June, and Nextel this fall. Verizon and Sprint will provide those same services not later than 2006. Again, we will provide all of this to you upon request.

Ms. MCCARTHY. Well, it is 2004, and let us hope it does not take until 2006, sir. I very much appreciate your enthusiasm on this issue.

General LIBUTTI. Yes, ma'am. I appreciate it.

Ms. MCCARTHY. I yield back.

Mr. PASCRELL. Mr. Chairman, would you yield for 30 seconds?

Mr. GIBBONS. The gentlewoman's time has expired, but without objection, we can yield to you for 30 seconds.

Mr. PASCRELL. I just listened to the conversation, and there is a zero amount of money budgeted for interoperability. So we are talking out of both sides of our mouth here, before we go any further. Thank you.

Mr. GIBBONS. Very good. Mr. Secretary, you do have an opportunity to respond to the comment since it was made.

General LIBUTTI. Well, sir, again, at the risk of beating a dead horse, my charge is the Intel piece and the infrastructure protection piece. I am very confident, having testified Tuesday with Dr. Chuck McQueary, that he and his folks are indeed on top of the interoperability science and technology application to help first responders.

Mr. PASCRELL. It is still zero.

General LIBUTTI. Sir, I will share with Dr. McQueary your concerns.

Mr. CAMP. [Presiding.] The Chair now recognizes the gentleman from Connecticut, Mr. Shays.

Mr. SHAYS. Thank you very much. Mr. Secretary, I was looking at your bio and I was thinking we are very fortunate to have you, and I was thinking of all of the other folks like yourself who want to be of service in this Department. I also was thinking, as our former chairman was there, he helped initiate the effort of the Department of Homeland Security, it came before my subcommittee when we established it, and it is amazing how much has been accomplished in a short period of time.

But my questions are—so when I ask these questions, I want to put them in the context of we have come so far, but we have so far to go. I also want to say that we had your Department—your part of the Department represented last year and it was a very unfortunate dialogue. We learned you had not yet been—the analysis side had not yet had their facility, we learned that there were not many people. You have Information Analysis and Infrastructure Protection. Under Information Analysis, how many people do you have?

General LIBUTTI. Again, I will look through my notes. I think we are just short of 90 people, sir.

Mr. SHAYS. Okay. That is an approximate; much better than where we were.

General LIBUTTI. Oh, yes, sir. Again, as you said earlier, I am a team player, Coach—

Mr. SHAYS. I do not want to spend too much time on that. You are much better than where you were. So can we leave it at that?

General LIBUTTI. Well, with all due respect, I just again want to signal to everybody that I look at it as one team. For dissecting organizational tasks, it is IAIP Op Center. I have, as I said, my total number—.

Mr. SHAYS. I am running out of time here. I am sorry. You have made your point. I do not think you need to make it again.

General LIBUTTI. Yes, sir.

Mr. SHAYS. But what I want to do is I want to get into the warning system. It is one part that you have, and I want to ask you right now, are we at green, blue, yellow, orange, red; low, guarded, elevated, high, or severe? Where are we at right now?

General LIBUTTI. Sir, as you know, during the holiday period—.

Mr. SHAYS. I want to know right now. Where are we at?

General LIBUTTI. We are at yellow, sir.

Mr. SHAYS. Right. And the reason I am asking that question is why are we at elevated? Why are we at elevated instead of guarded?

General LIBUTTI. We are at elevated because as those of us in the business of intelligence analysis, making recommendations and advice and protecting the homeland, there is absolutely zero doubt in my mind that the intent of Al-Qa'eda and other terrorist groups has not changed and they are hell-bent on bringing the country down. They have talked about, and we have collected information that indicates that they—.

Mr. SHAYS. I hear you on that. Explain to me, though, if you could, why would that not be the general risk of a terrorist attack?

What concerns me is you are already at that level of yellow, so you only give yourself one before you go to basically red. And I just wonder, because I feel right now that we are functioning under a guarded position, that there is a general risk of a terrorist attack, and I think that is how the public is functioning. We all know there is a general risk. I guess what I would love to know is whether—and I would like you to review that on whether we should not be back down one level. Because when you go to orange, my point is, and I am getting to this point, when you go to orange, you are basically saying that there is a high risk of a terrorist attack. But the same message we are getting out of your Department is, it is a warning to the people who can protect us, but it is not a warning to the general public, and I do not understand why when we go to orange it should not be a warning to the general public. I can understand if you went from—I am sorry, just from basically guarded to elevated, you know, but when you go to high. So if you could tell me why.

General LIBUTTI. My first step moving to answer your question, I ought to start by sharing with you my view relative to the two

points you made. You talk about risk and you talk about threat. The threat is the threat, and I talked about that by saying there is no doubt in my mind that intent has not changed. The threat is serious. We see actions that reflect that overseas. That is why we see the administration and our great, beloved military taking all appropriate actions to charge on a second front and bring people to justice, et cetera, et cetera.

But when you hold up risk assessment and the vulnerabilities that we identify when we look across the country at what I call centers of gravity and key target sets, and then we, with our friends and partners and industry and local and State authority, take those actions, preventive, protective actions, you take a risk—excuse me, a threat, you take actions, and you reduce the risk to those facilities and the American people. You do not take a threat and apply it to a situation. If you have taken measures and call that threat when you see it a 10, you call it a 10 when it gets to a target set. I am trying to define in simple terms the difference between ongoing threat, terrorist intent, and how we mitigate that threat by taking action.

Mr. SHAYS. I am trying to understand why we are at elevated as opposed to guarded.

General LIBUTTI. We are at elevated, sir, because the threat is real. The threat is real.

Mr. SHAYS. But wouldn't the threat be real if we were at guarded?

General LIBUTTI. Well, I think again, the gradations, the—if I could say the "shades of color" would simply indicate the requirement to be more aggressive in terms of—.

General SHAYS. I am just going to then renew my point. I would love you all to look at this a little differently. I think when you—we are going now in a guarded way. That is how the public is functioning. I think even that is how a lot of our local folks are. And I think you do not give yourself enough levels. And when you read what orange is, that tells me that it is more a warning not just to our law enforcement folks, but it also should be a warning to the general public. I do not think we should hear from the Department when we go to high that you should just do what you normally do. I think that is not wise, and I think it prevents us from doing responsible things.

General LIBUTTI. Sir, I hear you loud and clear and I appreciate your point, and I agree with you. I would only—if I may add a footnote. We do our very best to look strategically, operationally and tactically at what the threat means, we look at the actions we have taken and we try to assess what the risk is to a city, a county, a State, a facility. Again, I share with you parenthetically, having served in New York, this may be pretty sensitive to this next point. Our job is to share that information with State and local leadership, governors, mayors, our police chiefs, not to tell them how to suck eggs in terms of whatever decision they decide to make relative to actions in that place, particularly involved in communicating the threat in that city or region to the people of that area.

Mr. CAMP. Thank you, Mr. Secretary. The time has expired.

The gentleman from New Jersey, Mr. Andrews, is recognized for 8 minutes.

Mr. ANDREWS. Thank you, Mr. Chairman.

Thank you, Mr. Secretary, for your time.

General LIBUTTI. Sure.

Mr. ANDREWS. If a State trooper in Ohio stopped a car along Interstate 80 right now and the driver of the car was on the terrorist watch list maintained by the CIA, would the State trooper know that?

General LIBUTTI. Well, he does not know it instantaneously, sir. What he does is, through his dispatch, gets back to the terrorist screening center. The terrorist screening center will provide appropriate inquiries to a database or to a watch list—.

Mr. ANDREWS. I would assume so. Let us assume that it is an ordinary vehicle stop, just for speeding. The trooper has no idea of anything other than that. And let's assume for the moment that the trooper has a laptop in his or her car for local law enforcement purposes. Would the laptop give the trooper information to the terrorist watch list?

General LIBUTTI. You present an interesting scenario. Given the threat across the country, and from what I know police departments have done in educating and training and making their cops aware, I would put money on the fact that that cop would be very suspicious relative to any incident or situation of that nature and probably mind his manners, quite frankly, in terms of privacy and civil rights. But he is going to be as aggressive as he needs to be to follow up on what his intuition and professional training has indicated he needs to do.

Mr. ANDREWS. I agree with that, and I think that is very characteristic of police officers and I am grateful for that. But would the officer have access to the CIA watch list?

General LIBUTTI. The officer—again, I am sharing with you a process, sir. If he is concerned and wants an inquiry into the watch list or database, there is a system in place to do that and, normally, he or she would contact their dispatcher electronically back to the terrorist screening center in minutes, not hours; there is a turnaround of that information, and the gentleman or lady on the beat makes the judgment.

Mr. ANDREWS. See if you can walk me through that. So let's say the trooper, if the trooper had some reason to suspect that he or she should ask the question, the trooper would have to either e-mail in or call in to the dispatch.

General LIBUTTI. Probably call in or if they have a computer within the vehicle, they would use that system.

Mr. ANDREWS. Does the dispatch have the authority to get the information from the terrorist watch list? Does the Ohio State police dispatch?

General LIBUTTI. Yes, sir, again, following the process, following the procedures.

Mr. ANDREWS. What are the procedures? Tell me what happens between the dispatch and the terrorist watch list. What hoops do you have to jump through?

General LIBUTTI. I am not sure, sir. This is difficult or challenging, as you might think. But again, in simple terms, the cop on the beat works through his operation center, probably electronically nowadays, that information is passed back to the terrorist

screening center that is really the advocate and single point of contact for the cop on the beat. The terrorist screening center exercises its responsibilities and makes inquiries into watch lists or the database status, whatever that may be, does appropriate—asks appropriate questions, gets the answers and passes it back to the cop on the beat.

Mr. ANDREWS. How long does it take?

General LIBUTTI. I think it depends on the situation. It is—.

Mr. ANDREWS. What is the shortest time, what is the longest time?

General LIBUTTI. I will get you that information in terms of all of what I have indicated where over 1,000, I think I said earlier, 1,388 calls made and 527 positive matches. I would be happy to do two things, sir: give you whatever specific data we have, and two, provide you with appropriate slides, a detailed briefing on the interaction of the terrorist screenings.

Mr. ANDREWS. I would like to know the time range, what is the shortest period of time, what is the longest period of time.

General LIBUTTI. I would be—it would be premature for me and not wise to tell you 5 minutes, 6 minutes.

Mr. ANDREWS. Sure.

General LIBUTTI. I think it truly and very sincerely depends on the situation, circumstances. One of the points I made earlier when first questioned on this caused me to respond in a way that I will just again summarize. We are making a valiant effort and a noble effort to purify watch lists. Same name, same initial, different date of birth, other complicating details. That is part of the challenge, but it is working to purify watch lists and bring those watch lists into a database. That is going very well.

Mr. ANDREWS. Let me ask your opinion about something, and I ask this question without prejudice.

General LIBUTTI. Yes, sir.

Mr. ANDREWS. Do you think the day should come when an officer has on his or her laptop the watch list, has access electronically to it? Should that trooper be able to enter in whatever identifying characteristics he or she has of the stop and just get the information instantaneously?

General LIBUTTI. I think that is a terrific question. I would be prone to, given my background and experience, to take it on board and bring in duty experts from the police department and kick it around, as well as those charged with safeguarding extremely sensitive information and making every effort because of this great challenge we have of maintaining the balance between privacy and civil rights, individual rights as well. I would just want to make sure whatever system we put in place was darn near perfect in terms of protecting individual rights and privacy, and that we need to be very, very careful with all of that.

But the operational response is when in doubt take appropriate police action to safeguard the country and the American citizens. So again, I would be very happy to provide you details on this through my staff. Again, the FBI runs this. We have provided the Assistant Director For the Terrorist Screening Center, and we will contact him and pry out additional details.

Mr. ANDREWS. I appreciate your concern about civil rights, and I certainly share it. I do not think that anybody should be restricted in their liberty if we just are suspicious of them. That is not our law, that is not our tradition. But I also think that if there is a significant body of evidence that someone is being watched, that law enforcement officers ought to know that, because it is a piece of the puzzle that they can help put together—.

General LIBUTTI. I agree with you, sir.

Mr. ANDREWS. That might help prevent a catastrophe.

General LIBUTTI. You are right, and while what I am going to say does not support your example, I can tell you from my experience again with NYPD, the people who know the community and the area and the cops and first responders, it is not the guys at the Federal level, and that is why this partnership is so critical.

Mr. ANDREWS. It is also why I share Mr. Pascrell's view: we have to get some money in the budget for interoperability. I know that is not your call, but it is really important. Thank you, Mr. Chairman.

Mr. CAMP. Thank you. The gentleman from Arizona is recognized for 5 minutes.

Mr. SHADEGG. Mr. Under Secretary, thank you for your testimony today. I appreciate it. It is helpful to us.

I want to follow up on that line of questioning. I think we are all interested in actually the two-way communication between you and the cop on the beat and between the cop on the beat and you. In a minute I want to go into some staffing levels and find out how adequate you feel you are staffed, which I understand you have touched on already. But first let us talk about the question that was just raised.

In response to the issue of whether or not the officer on the street should be able to get on his laptop and access this list, you said that you would talk to experts in the field and analyze that issue and express your concern about privacy, and I think there is a valid concern about privacy. My question of you is, are you currently discussing, or do you have an ongoing analysis effort, to look at how functional that line of communication currently is; that is, we hear from our local police, look, you know, we cannot find out who the terrorist is; we worry that we might stop a terrorist and let her or him go. We are not sure that we are getting communication from the Department on these issues.

So I guess my first question is, hopefully a softball, are you guys studying this? Do you have an ongoing effort working with local police and State agencies to try to find out what would work, and how fast does it have to be to be functional?

Generalal LIBUTTI. The answer is absolutely, sir, yes.

Mr. SHADEGG. So it is a softball, good.

General LIBUTTI. Seriously, I mean again, you have to understand, I say this with great humility and respect for law enforcement and first responders. I mean this is where it is happening. That is where they are going to interrupt, disturb, detect, bring to justice these folks, so I mean my head and heart are there.

Back to the point about direct communications. Let me give you the Frank Libutti Marine Corps response to that and understand it in terms of now my greater responsibility as an Under Secretary.

We need to streamline communications, but we do not need to be cavalier or bullish in the way we do that, because there are lots of people who have equities in terms of dealing with the threat of terrorism.

I mentioned earlier, I believe I mentioned earlier that I am very much a supporter, and it would not surprise you given my background, in what I call chain of command and chain of communications, and I do not want to cut out people within that chain, particularly if we are dealing with an imminent situation. You stop somebody, things do not look good, it is going south in a hurry, this could be something big, or it could be a routine pull-over perhaps with someone who is involved in supporting terrorism, but indirectly through money handling, laundering, et cetera. We need to be very careful about that. And the answer to that question I think is broadly speaking, conceptually, streamlined communications is a two-way street. Get it to people who have to take action. Track that so that we get a good sense of warnings, indicators, and profile. It all talks to surveillance and counter surveillance programs that we do not run per se, but the cops on the beat do.

Mr. SHADEGG. Let's flip the coin. On the opposite side of the coin—well, one side of the coin are their concerns that they may not know they have stopped a terrorist, they want to be able to find out, they want to be able to help in the cause. The flip side of it is they have observed something suspicious, they want to pass it up the chain. And we get the same complaint there, that and colleagues might get—I suspect they do, I know I do, and complaint might not be the right word; concern there, about well, we are not sure if we passed it up if it would go anywhere.

General LIBUTTI. I would hitchhike on your point because it is a very good point and one that concerned me tremendously in New York as well. To that point, as I said earlier, we rolled out this homeland security information network. The guts of that is something called JRIES. JRIES is the Joint Regional Information Exchange System. We did not give birth to it; it was something within DOD months and years ago. I used it in New York. When I came down to Homeland Security, I said let us look at that to see if we can broad base this thing to support first responders. We are now doing that. It is extremely effective. The future in my view calls for us to integrate and complement other network systems. But the current system right now, where it has been embraced across the country, right now, with a view towards providing to 50 States and 50 other high urban areas within several months, these systems, this laptop system, this interactive system will give people on the beat the opportunity of darn near zero time response. As soon as you hit it, click send, that is gone, and that now, from the standpoint of that which is in New York City, is reflected in our operations center on a broad screen. We know what they know. We pass it back to them. We share it with all other members that are involved in the JRIES homeland security network right now. So the guy in California knows what the input is Newn York has provided, and that goes across the country.

Mr. CAMP. Thank you, Mr. Secretary. The gentleman's time has expired.

The gentleman from New Jersey, Mr. Pascrell, is recognized for 8 minutes.

Mr. PASCRELL. Thank you, Mr. Chairman.

General you talked about wireless in response to some questions before, and I am not going to bring up the subject about what is budgeted, because that is maybe beyond someone's pay grade, I do not know. But I understand that. You are the messenger. But you are more than a messenger down on Nebraska Avenue. You are more than a messenger. Because you spoke in your entire presentation to the question about commercial entities.

Understand that we are very concerned on this committee with public institutions, and that is why the subject of our first responders, police and fire, has been brought up. This is a critical issue. We are kind of flabbergasted as to the budget response. That was the whole point of the discussion, and I hope you understand that. It was not meant to be in any manner, shape, or form critical of you.

General LIBUTTI. I understand, sir. I appreciate your comment.

Mr. PASCRELL. Second point. You, throughout your presentation in terms of work that has been submitted, indicate, even in the area of personnel, not only service, but personnel, the hiring of personnel, you contracted out much of, a lot of this work. In fact, in many areas there is more contracted personnel than there are public personnel in terms of full-time equivalent employees.

General LIBUTTI. Correct, sir.

Mr. PASCRELL. My question is this, a very simple question: is this public record?

General LIBUTTI. I believe it is. I am a little, not taken aback, but perhaps do not understand your question as I should.

Mr. PASCRELL. Let me be more clear. In other words, anybody on this committee would be able to review any of the contracts that your agency has developed in terms of either service or personnel?

General LIBUTTI. I do not see why not, sir.

Mr. PASCRELL. Okay. So we would know who the private contractors are that you have looked to?

General LIBUTTI. The only concern, not in this forum, but in the appropriate forum in terms of specific manpower within the IA side, the Intel side, we need to be careful to share that at the appropriate classified level, and I am happy to do that.

Mr. PASCRELL. I understand your function and the function of your agency in terms of information-gathering and analysis, is to attempt to anticipate and then interrupt. I am simplifying it, and if I am incorrect, interrupt me.

General LIBUTTI. Well, forgive me for interrupting, and I only would add to what you have said, sir, to support you. It is about prevention, and then interrupt, deter, reaction.

Mr. PASCRELL. That is very interesting. Very briefly, the question of your agency, therefore, is not reactive. It is a—if we know a series of threats exist, we may suggest, we may not only try to interrupt those threats; we may act to try to remove the threats in the future. Therefore, this is more of a wider scope of involvement of your agency, of socioeconomic factors, groups that we interact with in other countries, so that we prevent these things from happening to change people's perception about America.

General LIBUTTI. Yes, sir.

Mr. PASCRELL. That is not an overstatement, is it?

General LIBUTTI. It is terrific, sir.

Mr. PASCRELL. Now, 2 years after September 11, we still do not have, and you have heard this today, our infrastructure risk assessment in terms of spending priorities, et cetera, et cetera. Can you tell me when this will be complete? Ranking Member Turner referred to this in one of his questions earlier today. And then give us a brief explanation as to why this is the case at this point.

And then I have one other question, if I may.

General LIBUTTI. What I would like to open with is a comment that is meant to again communicate my sincerity and yet my energy in moving forward. The magnitude and scope of the challenge ahead is such that assessment, risk assessment, categorizing vulnerabilities, and taking action will be a never-ending process and program. I would say again, since I have been on board, since early July as sworn, we have made great progress in this in terms of looking across the country, using indicators and lessons learned from Liberty Shield and in concert with the private sector, State and local officials, to begin this grand effort, this noble effort to put our head into and arms around critical information. It is an ongoing effort.

A week ago, I was privileged to be with the lieutenant governor in Virginia, and he grabbed me in the elevator and said, Frank, that list of critical infrastructure just is not right. And I said, yes, we have recently reviewed it and it needs to be updated and we are hard-charging to do that.

The point I am making, sir, with all due respect, is that this is a tremendous challenge, one that will never go away in terms of, you take your pack off. So I would simply tell you that there is an ongoing, aggressive effort to look at the top priority target sets and take protective action in terms of working with the private sector.

Mr. PASCRELL. One more, General. Please follow me.

Before 9/11, there was intelligence that went from Federal agencies, CIA, FBI, to the FAA about individuals, specific individuals that we were targeting, focusing on. We do not know clearly, and maybe the 9/11 Commission will bring this forward, we do not know clearly whatever happened to that information from the FAA, and I am sure they have been questioned on this, and we will learn about this. We know just very little.

How often do you actively communicate with senior intelligence officials from the CIA, the FBI, the DOD, the State Department, to go through difficult interagency problems such as information-sharing, and defining lines of jurisdiction. There are a lot of questions at least hinting to that. Do you ever meet as a group, for instance?

General LIBUTTI. The answer to all of those questions is yes, yes, and yes. I talk to folks every day in the Intelligence Community across those agencies. Pat Hughes, General Hughes, the Assistant Secretary for Intelligence, talks to TTIC several times a day, the FBI, the CIA, DIA, State Department contacts. And others across the Federal Government. Pat Hughes holds within the Department of Homeland Security meetings every month with members of the intelligence team in the Department of Homeland Security.

Now, let me pause and tell you what I mean by that so you get a good sense. When we brought all of the agencies together, they came in, they had their operational element, and they had their Intel teams to support their mission profile. This had not gone away, and properly so. Pat Hughes, as the Intel officer for the Department of Homeland Security, has exercised his leadership in tremendous fashion, bringing together the leadership and the intelligence business across the Department, and he does that regularly. That reinforces the notion that the center of gravity, the center of the universe in terms of advice and sharing information at a senior level is happening repeatedly, very aggressively, and productively.

Mr. CAMP. The gentleman's time has expired.

Mr. PASCRELL. Thank you.

Mr. CAMP. Thank you.

Mr. Secretary, looking at the IAIP Directorate as a whole, can you give some examples about how the information-sharing and intelligence programs are aiding this critical infrastructure protection effort?

General LIBUTTI. Sir, I can, and I shall. I would tell you, as I mentioned in the opening statement about the Information Operation Center, and I will try to again summarize this and then I will respond to additional questions.

The centerpiece of what I do is information-sharing/intelligence. The other piece of that, is to take appropriate action to protect the infrastructure of the country and then advise appropriate leadership.

Key point: information-sharing. The operation center for us, and I am privileged to tell you that General Matt Broderick, retired Marine works for me. He runs the operation center. But he is in charge of the Secretary's operation center and not my operation center. That operation center is indeed, as mentioned earlier, the nerve center for communications. And in that regard, it is through the operations center that inquiries are made, advisories, bulletins, and alerts to our customer base across the country are sent out and received. In addition to that, there are frequent conference calls, secure VTC with our friends at the White House, other members of the interagency, and State and local officials as well.

The operation center conducts itself on a 24/7 basis. It has representation as liaison to other organizations to help with information flow and sharing of that information. So you have agencies represented in the operations center from Federal Government organizations, DOD, FBI, State, local police. During the holiday period, we had detectives from NYPD and California sitting with us. During the holiday period, given the threat and the credibility of that threat, under our leadership in IAIP and the blessing of the Secretary, we sent executive teams to several locations across the country to meet with mayors, governors, police chiefs to share with them real-time, face-to-face what we knew about the threat and recommendations that we thought should be put in place. It gives you a broad overview of how important information sharing is.

I would only add this footnote, and I am repeating myself. The guts of what we do in terms of the Web-based connectivity stream is the homeland security information network. That is good to go

now, will improve in terms of the expanded capability in the future. The JRIES program, the guts of that worked very well. In the future, this homeland security network in terms of sharing critical IAIP information will go from unclassified law enforcement-sensitive by the end of the year to a classified, secret level information-sharing system.

Mr. CAMP. To follow up on that, I have seen figures that 98 percent of our critical infrastructure is in private hands, and clearly there needs to be a collaborative effort between the Department and the private sector, and I know that the ISACs, the information sharing and analysis centers, have been created to share information on threats and vulnerabilities. I wonder if you could just comment on the progress those have made. I realize there are some challenges that remain, particularly communicating with industry on activities being set up by the Department and other items.

General LIBUTTI. Yes, sir. It gives me a good chance to brag a bit on the leadership and aggressive spirit of Bob Licouski, Assistant Secretary for Infrastructure Protection, who has my full confidence and is indeed charging ahead. I want to comment a little bit on this ISAC business so you understand how I feel about it.

This organization or group of people is absolutely central to information sharing and the high expectation we have that they will be leaders within the industry to bring the industry together, not simply to pass information. Having said that, Bob is looking on my behalf into how we can look at ISACs and broaden their capability and responsibility as true capital L leaders in the community. We think they can do more. We think they have done a super job. But we need to, I think, reorient perhaps their direction and their influence.

To that point we have brought together what is called the ISAC Council, made up of senior representatives across all communities, and we are posing that very question to them, soliciting their advice. But we are focused on improving what is now a good system and making it an outstanding system. So again, key point. They are critical. They have to play. We are looking at ways to make their contribution even greater.

Mr. CAMP. Thank you. I see my time has expired.

The gentleman from Rhode Island is recognized for 5 minutes.

Mr. LANGEVIN. Thank you, Mr. Chairman.

Good afternoon, Mr. Secretary. Thank you for being here.

General LIBUTTI. Yes, sir.

Mr. LANGEVIN. Let me begin by following up on some of the things that Chairman Cox and my colleague Mr. Pascrell have already touched on.

As you can tell from the questions that are coming from the committee, there is still a great deal of concern, even confusion, over the relationship between DHS and the rest of the Intelligence Community, and I am sure there is probably going to be a recurring theme until we are confident that that relationship is seamless. We ask for obviously your cooperation and your indulgence in trying to work with us to get through this.

But in particular, my question centers on the creation of TTIC and the terrorist screening center, which perhaps seems to again

have muddied the waters when it comes to the roles and responsibilities of key counterterrorism units.

So my question is, and perhaps you have already answered in some way, but do you share any of this confusion? Do you see any concerns that we should be aware of, and do you think it would be helpful to have a written presidential directive clarifying the roles and responsibilities of IAIP, TTIC, TSC, CIA, FBI, and the rest of the Intelligence Community?

General LIBUTTI. I have already made the comments in response to your question to other members, and if you will permit me, I will sort of summarize that as opposed to going through a long list of that which I think is critical, but I will be prepared to stand by for that, sir.

We are a new organization. My feelings, and I am a guy who sees things half full, not half empty. If I get any sense from any member of the Intelligence Community that is not treating us with appropriate dignity and respect and understands that we are full players, I take appropriate action. And I have not hesitated in the past to do that.

Now I tell you that not to be so bravado, but to tell you as a footnote I have not had to do that much. I tell you that the leadership of the FBI, CIA, TTIC and the rest, including DIA, they get it. They understand the responsibility of the role that we shoulder.

Where there has been, if any, problem along the way is with some younger folks who do not understand the changing culture, perhaps have not read the Homeland Security Act, but when they are instructed, when they are coached, they get it. But I can tell you that for the time being at every turn we are going to have to ensure that we do not miss the opportunity to inform people of what my mission is, what the mission of Homeland Security is, and make darn sure they understand that this is a team effort.

So I do not know if that answers part of the question, but I have—I mean we do not live in a perfect world. I mean even great organizations across the country, the Federal Government, all branches of government, certainly would admit in an open and candid discussion that they can always make improvements to either the decision process, administration, logistics, whatever. And we are in the process of doing that. And you have my guarantee we will continue to improve the system. But the bottom line is the system is working. And I say that in terms of TTIC and the terrorist screening centers. Lord knows, it is only in its first phase of standing up and being fully operational. And I will be happy at any point in time to come back one-on-one or send my staff to meet with your staff, sir, to share with you the status of progress being made.

Mr. LANGEVIN. I guess one particular point, just in following up, is there any information that TTIC receives that DHS does not?

General LIBUTTI. Well, I need to be careful with that, and I say this sort of tongue in cheek, you don't know what you don't know. But I know what the Homeland Security Act says, and it says I have unfettered access to all intel.

Part of the challenge in the past and probably that which merited correction and we took it was when we started IAIP up—and I might add we just moved into a new building, and I invite you

all and your staff to come visit us. It is at the NAC. It is the same facility, but it is a renovated building.

Back to my point, initially, we did not have electronic connectivity with databases across the intelligence community. That has been fixed. So perhaps that is one of these small boulders that we circumvented to move forward; and we have done it quite well, in my opinion.

We are always looking for ways to improve, we always try to be better listeners, but we act, behave and expect respect from the intelligence community as full players.

Thank you, sir.

Mr. LANGEVIN. Thank you, Mr. Secretary.

I see my time has run out. I will forward another question to you for the record, basically asking you if you could explain what information DHS has collected from States and the private sector regarding risk assessments and describing how it is being used by DHS to build a priority list, but I will submit that to the record since my time is expired.

General LIBUTTI. We will be delighted to respond. Thank you, sir.

Mr. CAMP. Thank you, sir.

The gentleman from New York is recognized for 5 minutes.

Mr. SWEENEY. Thank you, sir.

General good to see you again.

General LIBUTTI. Good to see you, sir.

Mr. SWEENEY. As a fellow New Yorker, I will try to be direct and to the point, as you always are, and I am going to maybe beat a dead horse but continue down the same line of questioning, with the hopes that I think you understand it, but other people understand in the intelligence community—.

General LIBUTTI. I understand, sir.

Mr. SWEENEY.—the concern that we have over the ability of TTIC to incorporate itself into and be a useful process with a great deal of confidence being gained by Members of Congress and the American people, and I think that the key to that is—and I know the Chairman has mentioned this before. I was going to talk to you about personnel levels. I know you have answered those questions, and you are going to get back. But the key to this really is—and I want the world to understand it—that you have got to be the guy in charge. We all believe that here in this body, and I don't believe other people believe that.

I think there are some written comments that I would like to cite just because I am very concerned when I read them.

In a February 27th article on Fox News, John Brennan, the Threat Center Director, said, quote, do you really want to give this new organization, Homeland, the responsibility for setting up with secure communications systems and networks and having a fully trained, analytical cadre? No, you don't want that. What you want to do is tap into the capability that already exists.

Now, the latter part of that I agree with, but it seems to me that there is a public resistance to the ideas or the intentions that I think Congress had when we moved forward and established the Department of Homeland Security.

Later in the article, Vince Cannistraro is quoted as saying—and I know he is not (he is former, retired), but he is highly respected. Quote, it is a joke. What do you gain by having DHS intelligence?

Now we have been here before and seen this. It is culture. We get it. We all knew it coming into the process, and I urge you, I guess, to be blunt and be a New Yorker, to throw your weight around. You need to justify your contributions. You also need to justify why you need to be in the game in TTIC, and you will have a lot of support here on both sides of the aisle, I would point out.

I want to get to just very quickly some more ministerial or tangible kind of questions.

Providing State and local officials—other colleagues have asked this—security clearances, secure communications and storage—and we see resistance on just the broader sense, so this may be an impossible question for you. How are you going to pay for it? Is it all coming out of IAIP? Is it shared by somebody else?

General LIBUTTI. The appropriate response is that, initially, in support of the Homeland Security Information Network, that is $11 million to support 50 States and 50 other urban areas. It is a combination of monies. My recollection—my staff no doubt will pass me a note if I miss the mark on this, and I will share it with you, sir, but I believe it was—the lion share of that money came out of IAIP because we could afford to do it in 2004 and additional funds from the office of domestic preparedness, if I am not mistaken.

We think this is a great first move forward. We will look now, in terms of what I call the deep fight, what are we going to do in a couple of years in terms of this system. Given that technology is turning over so rapidly and my intention is to provide the first responders the best available, we have got to figure out—because this is nobody's, what I call in my own language, cost center line, that program money to support that, but it was an initiative we thought was absolutely critical. We moved out on it smartly, and it has been well received across the country thus far. The implementation of that will probably hit the street in early summer.

Mr. SWEENEY. Let me get to two real kind of tangible things as it relates. On the $11 million, what do you think the 2004 number is in terms of how many clearances you are going to be able to have successfully completed?

Secondly, I just left the Approps Subcommittee hearing with the Secretary, and this issue came up as well of the context of communicating between the varying levels of government.

I would like to work with your staff at identifying other resources that may be available both in and out of DHS, and to some degree that is a tough place for you to go, but we need to have some ideas. And, I think your partners in TTIC could be helpful in this, and it may be a suggestion that in the appropriations process we may be able to pursue. But, more directly, a ballpark number, how many local and State clearances you think you will have done by 2004, end of 2004?

General LIBUTTI. The short answer and correct answer is I don't know. The clearance piece and the funding for that is not coming out of my shop. I am not the lead for clearances, sir. I will take that back and put it in the right department.

Again, my job is, as you have heard me say, support the first responders, support our customer base, talk to the threat, deal with the infrastructure protection, but I will take that back.

Mr. SWEENEY. And we may need to strengthen that. There is great concern and has been great concern that first responders have been out of it, and you are the guardian angel there.

Mr. CAMP. Thank you. The gentleman's time has expired.

The gentleman from Washington is recognized for 5 minutes.

Mr. DICKS. First of all, I want to apologize for not being here for your testimony, because I am ranking on an Appropriations Subcommittee and was on a much less exciting issue than this, but thank you for your good work and effort.

Let me ask you a couple of things. In the new DHS strategy document—you may have covered this, but please bear with me—released last week, the Department says that it will have a complete database with a prioritized critical infrastructure list by the end of 2004. It is unclear, however, who is spearheading this work at an operational and analytical level within IAIP. Can you tell us who is spearheading that?

General LIBUTTI. Well, I am in charge of IAIP, and Bob Liscouski, as Assistant Secretary for Infrastructure Protection, is the lead for me in that regard, sir.

Mr. DICKS. Okay. Let me ask you specifically, have the States sent in a list of critical infrastructure? Because the State of Washington I know not only have they sent in a list, but they have got a plan. I believe each State should have the first crack at developing a list of critical infrastructure in their State and to come up with a plan and submit it to the Department. Now, is that being done?

General LIBUTTI. It has been done, sir. Plans were submitted including that information among lots of other things they submitted by our request. They were due the end of December. Plans were received. Washington's plan was absolutely superb.

Mr. DICKS. I couldn't believe how comprehensive it was.

General LIBUTTI. It was tremendous, and if we had time, I would show you all the plans.

But I would tell you this. One, some of the plans were sent back for tweaking to help us help them, but the plans are in. The Secretary appreciated it tremendously, and it is the first step forward in what I used to complain about—let me restate that. My concerns in New York were that—and they fixed this, by the way—that the need for a strategic plan that brought together cities and towns across New York State with a focus on priorities, with a focus on ecumenical approach to the challenges at hand that dealt with money, that dealt with how we deal with that which in the infrastructure category really needed to be top, top priority.

So I am absolutely delighted that the States, based on the leadership of the Secretary, Secretary Ridge, have supported this business. A strategic plan is the basis to bring the country together in terms of looking at resource requirements, prioritization, a blueprint for moving forward. I mean, I applaud it; and, again, I recognize the great work—.

Mr. DICKS. Good. My time is very short here, so I don't mean to cut you off. Are these plans going to be utilized by your Depart-

ment in developing this database? I certainly would hope they would be.

General LIBUTTI. Sir, the name of the game is—am sure you have said this a million and one times in the leadership you demonstrate every day. It is about partnership, and we will use all of the information within those plans to frame, to shape and to make appropriate decisions on infrastructure, on intelligence, information sharing and in any other area in my directorate that I have responsibility for.

I would tell you that in the infrastructure business what we have realized is you have got to look at the physical and the cyber; and what I have learned in the 6, 7 months I have been with the Department is that there is incredible interdependency across industries. You can think of any one industry and think about if you had catastrophic failure in one industry, what would the impact be on the other and how would that affect the small towns and big cities and the industry at large across the country? So I am with you a hundred percent, sir, and I appreciate it.

Mr. DICKS. The other thing is on the national cyber security division. You know the President has laid out his vision here, the national strategy to secure cyberspace. But is it being properly funded?

It says the President's budget requested $60 million for its information warning and advisory program. This program has three core components: tactical indications and warning analysis, information requirement management, integrated physical and cyber structure monitoring and coordination. With the exception of $56.6 million allocated for the information warning and advisory groups for the live wire cyber exercises conducted by NCSD, the budget request does not specify how much of this total is allocated for cyber security. Can you, for the record, give us an indication of how this is going to be funded?

General LIBUTTI. Yes, sir, I can. In the 2005 budget, the information warning advisory is $23.7 million, and the remedial protective action program and support of cyber is $55.9 million.

Mr. DICKS. And you have said—going back on the infrastructure—the database will be completed by the end of 2004. Is that calendar year or fiscal year?

General LIBUTTI. Say the statement again, sir. The end of 2004?

Mr. DICKS. Yes. It says a complete database with a prioritized central infrastructure list by the end of 2004. The Department says that it will have it complete.

General LIBUTTI. It is by the end of the calendar year, sir.

Mr. DICKS. All right.

Mr. CAMP. The gentleman's time has expired.

I want to thank the Secretary for being here. This joint subcommittee hearing is now adjourned.

General LIBUTTI. Thank you very much, sir.

[Whereupon, at 12:09 p.m., the joint subcommittee was adjourned.]

APPENDIX

MATERIAL SUBMITTED FOR THE RECORD

PLEASE: NOTE: UNDER SECRETARY LIBUTTI DEPARTED DHS FEBRUARY 1, 2005. MATTHEW BRODERICK, THE DIRECTOR OF THE HOMELAND SECURITY OPERATIONS CENTER SUBMITS THE FOLLOWING RESPONSES ON BEHALF OF DHS.

QUESTIONS FOR THE RECORD FROM THE HON. JOHN B. SHADEGG

Undersecretary Libutti, the State of Arizona is establishing a fusion center for intelligence this May that will be officially called the Arizona Counter-Terrorism Information Center.

Question: 1. Are you aware of this effort?
Answer: Yes, we are aware of Arizona's establishment of a fusion center for intelligence. Many of the States are setting up similar entities. We are working to develop a coordinated effort and standards to provide guidelines for all states wishing to establish information centers. This is one of the top priorities of the DHS Information Sharing and Collaboration Program, and the. Office of State and Local Government Coordination and Preparedness.

Question: 2. How will the Department of Homeland Security interact with this Center? Will it have direct two-way communications?
Answer: The Department of Homeland Security has established communications between the Homeland Security Operations Center (HSOC) and all states via the Homeland Security Information Network (HSIN). We plan to strengthen these communications by providing connectivity up to the secret level in the future. To date, eighteen Law Enforcement Intelligence Centers or Fusion facilities have been identified to receive Secret level capability packages to operate at the collateral level. Facilities identified as key coordination and fusion centers by each state and that have been constructed to handle classified information will have priority.

Question: 3. Have other states created similar centers?
Answer: Yes, other states have created similar centers, based on state or regional requirements and relationships. The Department of Homeland Security, through the Information Sharing and Collaboration Program, the Office of State and Local Government Coordination and Preparedness, and the DHS Operations Center, is working to develop an interconnected and collaborative partnership between both DHS and each of these centers, and between and the State centers and any regional centers which may develop through consortium efforts of the States.

Question: 4. If so, are there any lessons to be learned from those efforts before Arizona's Center is officially opened?
Answer: The Department of Homeland Security has a team scheduled to visit Arizona this month. We will use this opportunity to provide advice and establish connections between Arizona, as well as other states.

Question: 5. In the Fiscal Year 2004 Homeland Security Appropriations bill, there was $10 million in funding to the IAIP Directorate for a command center and emergency communications network. The National Alliance of State Broadcasting Associations will soon complete an AMBER Alert network that could potentially be used for an all-alert network. How is the Directorate using that funding?
Answer: Using 2003 & 2004 appropriated funds, IAIP implemented the Homeland Security Operations Center (HSOC) capability. The HSOC is the primary national hub for domestic incident management operational coordination and situational awareness. The HSOC is a standing 24/7 interagency organization fusing law enforcement, national intelligence, emergency response, and private sector reporting. As such, the HSOC facilitates homeland security information-sharing and oper-

ational coordination with other Federal, State, local, tribal, and non-government Emergency Operation Centers (EOCs). Further, the HSOC is the primary conduit for the White House Situation Room and IIMG for domestic situational awareness.

QUESTIONS FOR THE RECORD FROM THE HON. MAC THORNBERRY

Question: 6. How is private sector interaction being coordinated and funded within the Department, particularly with the operational arm of the private sector, i.e., Information Sharing Analysis Centers (ISACs)? Who in the Department is responsible for coordination, but as important, program management and budget oversight of these varied initiatives? During your testimony, you mentioned that the ISACs may need to be re-directed in their efforts—what specifically does this mean, and what direction are you recommending for the private sector? Will the NCS funding model for the telecommunications ISAC, as noted below, become a model for other sectors to strive towards?

- We are aware of a newly established TSA encrypted web-based communication system called the Maritime and Land Security eCOMM (MLS eCOMM) that will provide for the real-time exchange of Alert Bulletins, Best Security Practices, Program Initiative Information, and Guidance and General Information.
- We are aware that IA recently announced the Joint Regional Information Exchange System (JRIES) that will provide secure communications for state, local, and private entities.
- We are aware of the NCSD Cyber Alert and Warning system, also a web-based communication system.
- The National Communications System (NCS) has already spent millions for the Cyber Warning Information System, a secure out-of-band collaboration system.
- In addition, the NCS fully funds the National Coordination Center which serves as the Telecommunications ISAC for that sector, which is staffed by government and private sector individuals.

Answer: Within IAIP, the National Infrastructure Coordinating Center (NICC) maintains operational awareness of the nation's critical infrastructures and key resources, and provides a common infrastructure for information sharing and coordination between and among government, critical infrastructure owners and operators, and other industry and private sector partners. DHS has developed and is implementing a plan to integrate the referenced systems into the Homeland Security Information Network (HSIN). The HSIN is a secure, unclassified backbone communications network that offers a conglomeration of "communities" and information management tools. It provides a common platform for communication with law enforcement, and state and local government. DHS is in the process of deploying the functionality of HSIN to the critical infrastructure and key resource sectors described in HSPD–7. Currently, these sectors have varying levels of information sharing capabilities. HSIN will provide core capabilities to bring every sector up to a baseline of information sharing features, which includes extending the ability of sectors to deliver alerts, warnings and advisories to more members at little to no cost to them. It is intended that any future information sharing system implemented by DHS will be an integrated component of HSIN. The Infrastructure Coordination Division, within IAIP, is responsible for coordination and integration of these initiatives as they relate to the CI/KR, and ensures coordination and addresses issues with and between the CI/KR sectors. The HSOC provides oversight to the HSIN. For the Telecommunications Sector, the NCS National Coordinating Center (NCC) for Telecommunications functions as the Telecom Information Sharing and Analysis Center (ISAC). This joint Government Industry collaborative body established in 1984 builds on the history of cooperation and established trust relationships to address the initiation, coordination, restoration, and reconstitution of national security/emergency preparedness telecommunication services and facilities under all conditions, crises, and emergencies. The NCS funding model will not be used for other ISACs. ICD will address each sector individually, recognizing that each has unique characteristics and needs.

Question: 7. The IAIP budget describes IAIP and the Homeland Security Operations Center (HSOC) as the principal mechanism for the execution of all DHS programs, with focus on federal, state, local and private sector systems. IAIP has requested an increase of $10 million for HSOC upgrades to include information sharing missions (providing a total of $35 million in fiscal year 2005). Is any of this funding going to be used to help the private sector integrate their information and expert analysis into the HSOC? If

not, how does DHS plan to work with the private sector as a caretaker of the critical infrastructure? Please provide description of specific projects.
Answer: Yes, in 2004, HSOC began the rollout of a national information sharing capability that is called the Homeland Security Information Network (HSIN). This network connects federal, state, local, tribal and private sector infrastructure stakeholders, enabling information sharing and collaboration within and among communities of interest. HSIN–CI (Critical Infrastructure) is a community of interest within HSIN that is dedicated to private sector components of the nation's critical infrastructure. A significant portion of the 2005 HSOC budget request is planned for growing the infrastructure and the reach of HSIN. HSOC is working closely with the Infrastructure Protection division of IAIP to identify and reach these private sector participants.

8. Cyberspace and the potential threat to our homeland through cyberattacks are of concern and priority for the Department. The Homeland Security Act calls for DHS to perform comprehensive assessments of cyber vulnerabilities (Sec 201 (d)) and carry out comprehensive assessments of the vulnerabilities of the key resources and critical infrastructure of the United States, including the performance of risk assessments (Sec 201 (d)). Risk assessment involves the correlation of threat and vulnerability to determine the risk to the nation, with IA responsible for cyber threat evaluation and IP responsible for cyber vulnerability assessment. The fiscal year 2005 budget requested $79.8 million to expand the capabilities of the IP National Cyber Security Division (NCSD), which according to the DHS "implements the public and private sector partnership protecting cyber security as it identifies, analyzes, and reduces threats and vulnerabilities; disseminates threat warning information; and coordinates cyber incident preparedness, response, and recovery efforts." However, there does not appear to be funding for cyber within the IA budget request for cyber threat analysis. There is also confusion on which of the "watch centers" has responsibility for overall cyber threat reporting, noting that the IP

National Communications System (NCS) operates a 24X7 telecommunications watch center, IP NCSD operates a 24x7 cyber watch center, and IA operates a 24x7 Homeland Security Operations Center. The U.S. Secret Service also operates a 24x7 watch operation for electronic crimes, which is a direct mission of cybersecurity. Each has a significant funding request, but there is little information available on how these watch centers integrate cyber information for national threat assessment and if there are plans for eventual integration of these watch centers into one cohesive unit.

- **Please describe how these different watch centers will be integrated to ensure efficiency and effectiveness in protecting our country from cyber threats.**

Answer: Currently the watch centers of the DHS/IAIP/IP divisions are physically separated according to function and division missions, but integrated in terms of information sharing. As DHS stood up, it was important that each division retain the 24x7 watch capabilities critical to their respective missions. During this time, each watch center has routinely collaborated with the others to share information and coordinate singular, integrated, and focused responses. Now that the divisions are more mature, IP will be integrating functions of the National Cyber Security Division's (NCSD) US–CERT, the National Communications System's (NCS) National Coordinating Center for Telecommunications, and the Infrastructure Coordination Division's (ICD) Watch into the National Infrastructure Coordinating Center (NICC).

Co-located with the Transportation Security Administration, the NICC will provide a coordinated and seamless information sharing capability with the IP NICC desk at the Homeland Security Operations Center (HSOC) and among all industry partners associated with critical infrastructures and key resources.

The U.S. Secret Service (USSS) has an Investigative Support Division duty desk, which supports its field investigations (cyber and otherwise) on a 24x7 basis. Relevant information from the duty desk is coordinated through USSS headquarters and through the HSOC.

- **How does IAIP interact with the Intelligence Community for classified cyber assessments? Does IAIP work with TIIC for cyber threat analysis? If so, how is this information shared within the department for analysis and warning, as well as correlation with vulnerability information provided by the private sector? How is cyber threat information shared with the private sector, and who has that responsibility—IA or IP/NCSD?**

Answer: NCSD is working intensively with the law enforcement communities as well as DHS/IA to develop a comprehensive threat, risk, attribution assessment and response capability.

NCSD interaction with the TIIC (in December, the National Counterterrorism Center (NCTC) undertook all functions assigned to the TIIC) is accomplished through DHS/IA, law enforcement and intelligence community detailees on staff in IAIP. With regard to classified assessments, the NCSD works with the Office of Information Analysis (IA) in the Information Analysis and Infrastructure Protection (IAIP) Directorate through our participation in IA's periodic threat assessment meetings and on an as-needed basis in the case of a particular threat or vulnerability. One example of this coordination was the participation of NCSD through IA in the National Intelligence Estimate' (NIB) "Cyber Threat Against the Information Infrastructure." This classified document is an update of the 2000 NIE. In addition to the regular meetings both IA and NCSD participate in daily conference calls with the National Security Agency/NSIRC, the Central Intelligence Agency, and the Department of Defense's Joint Task Force Global Network Operations (JTF–GNO) to discuss classified cyber activity of note.

Through its mission to serve as the national focal point for cyber security issues and to implement the National Strategy to Secure Cyberspace, the NCSD is responsible for managing and issuing cyber advisories and warnings. Those advisories and warnings are issued to the public and our partners through the National Cyber Alert System and to specific entities on an as-needed basis in the case of a targeted vulnerability or threat. Information that is less sensitive and for wider distribution is disseminated through the US–CERT public website and the US–CERT secure online portal, as appropriate. The Department also receives various intelligence reports regarding the world-wide cyber security situation, but because of the central role of the United States in the cyber world, the locus of effort and source of nearly all relevant assessments are activities led by the Department and its partners in the public and private sectors.

- **How does IAIP determine risks posed by particular types of cyber attacks, including assessment of probability of success, and feasibility and potential effectiveness of countermeasures?**

Answer: As mentioned above, risk assessment involves the correlation of threat and vulnerability to determine overall risk to the nation. With respect to cyber threats, the US–CERT has developed a threat severity rating scheme and identified countermeasures for degrees and types of cyber attacks. That scheme is a standard, repeatable and reliable method to assess the criticality or severity of new or emerging cyber security events. Once information is received about an actual or potential event, US–CERT assesses its "severity" using a scale from 1 to 5, with 1 being minimal and 5 being a crisis. Factors that are weighed in determining the 'severity' of a security event are based upon a matrix of factors, and appropriate countermeasures are considered.

From a strategic standpoint, the NCSD is developing a set of guidelines on cyber aspects of vulnerability assessment for the critical infrastructure sectors as part of the Homeland Security Presidential Directive 7 and Sector Specific Plan implementations. Once finished, those vulnerabilities can be mapped against potential and emerging threats to provide risk assessments.

- **How will the Cyber Warning Information Network (CWIN) that has been deployed by IP be integrated into the IA Joint Regional Information Exchange System (JRIES)? How are cyber warnings coordinated between IP National Cyber Security Division and the IA Homeland Security Operations Center?**

Answer: CWIN will be technologically and operationally integrated under the Homeland Security Information Network (HSIN) umbrella concept under the direction of IP/ICD. Within the HSIN network platform, CWIN will serve as the highly reliable back-up communications network component during crisis. The network is currently in use by selected Federal agencies, private industry, and Information Sharing and Analysis Centers (ISACs). Additionally, HSIN-Secret will use the CWIN network for collaborating collateral level information. DHS will work with the states and critical infrastructure sectors to identify nationally critical operations centers requiring CWIN connectivity to remain connected to DHS during a crisis. The Infrastructure Coordination Division (ICD) has created a prioritized implementation list of future CWIN sites. A draft Concept of Operations (CONOPs) and Standard Operating Procedure (SOP) has already been developed and once approved, would govern CWIN protocols and usage of the network.

JRIES represents a community of users that also sits on the HSIN network platform. Consequently, key participants of JRIES may have access to CWIN based on whether those JRIES participants meet the identified CWIN criteria for member-

ship. The US–CERT, through its HSIN web portal, which utilizes JRIES, routinely shares information with the HSOC on cyber security issues and alerts, including participation in daily conference calls and regular e-mail correspondence. CWIN, as the back-up network under the HSIN umbrella could have the capability to replicate data from the JRIES tool. In time of crisis when JRIES or other forms of communication are inoperable, DHS will continue its operations on CWIN. CWIN has extended connectivity to each State's emergency operations center (EOC). This was done, in part, to provide an interim solution which allows for the transmission of information up to the SECRET-level within and between the HSOC and the States' EOCs; this capability will be significantly expanded once the Homeland Security Data Network (HSDN) is fielded. Under this approach, CWIN would serve as the backbone network providing immediate connectivity to the States, with HSDN connecting through appropriate encryption devices to the state EOC offices.

- **How does DHS integrate cyber advisories and warnings into the existing Homeland Security Advisory System, given that cyber has a unique audience, particularly when those people who must respond to an attack are not the First Responders used for physical national disasters?**

Answer: NCSD provides information for use in the Homeland Security Advisory System to be activated as appropriate. However, the nature of cyber attacks is that there are varying degrees of cyber activity at any given time that warrant advisory to the cyberspace stakeholder community that does not meet the criteria for raising the national alert status. Therefore, US–CERT utilizes its National Cyber Alert System (NCAS) to let the stakeholder community know about activity that may warrant information protection measures but that does not rise to the national security level of the Homeland Security Advisory System. US–CERT is reaching out to key partners for incident response at various levels of sensitivity or urgency through the NCAS, the Homeland Security Information Network (HSIN)/US–CERT Portal, and the US–CERT public website to communicate with cyber "first responders" and other stakeholders.

9. I would like to have a better understanding of overall coordination of exercises within the Department. For example, IAIP has requested $1.9 million for cyber exercises in fiscal year 2005. FEMA's budget includes $20 million for planning and exercises associated with medical surge capabilities. The U.S. Secret Service conducts tabletop exercises, but the funding is not clearly identified for this effort.

- The Office of Domestic Policy manages a National Exercise Program for counterterrorism in support of Homeland Security Exercises—"TopoffI" and "TopoffII." TopoffI was conducted under the auspices of the Department of Justice. These exercises were conducted in Seattle and Chicago. TopoffII and subsequent exercises was/will be conducted under the auspices of the Department of Homeland Security (DHS).
- The Department of Defense will presently conduct a Homeland Defense exercise titled "Determined Promise '03 and Amalgam Chief 03–13", This robust command post and field exercise is the precursor/requirement for Northern Command's (NORTHCOM) approval for "Full Operational Capability (FOC)" status.
- The Secret Service Electronics Crime Unit (ECU) is reaching out to the private sector and supporting table-top exercises to address the security of private infrastructures, These have been extremely successful, as demonstrated during the recent exercise in Houston.
- The "Live Wire" exercise, sponsored by Dartmouth College, took steps to integrate the private sector into their cyber exercise effort, but there was very poor coordination of the overall exercise.
- TSA in coordination with the U.S. Navy War College is also beginning the planning for a series of exercises.

Throughout all these activities, there appears to have been little integration of active private industry/infrastructure into these exercises. Who has overall responsibility for coordination, and how are exercise results shared with other federal, state, and private organizations?

Answer:

Coordination

Secretary Ridge directed the establishment of a national exercise program following the conclusion of TOPOFF 2. He approved the plan in October 2003. The Department's Office for State and Local Government Coordination and Preparedness (OSLGCP) administers the Program, and is implementing it through coordination across government and by hosting a series of planning conferences to facilitate implementation. OSLGCP has responsibility on behalf of the Department to work with

DHS program offices and interagency partners to establish and administer the Program, provide policy and program instructions, and monitor, analyze and report on the progress of implementation.

Agencies, departments and offices serve as leads for national-level exercises and Program elements that fall within their specific areas of responsibility. The Program is designed to support and assist their efforts. OSLGCP works closely with participants spanning the interagency, all levels of government, the private sector, and international audiences, and with other DHS Directorates/Components. The Department's Operational Integration Staff coordinates departmental participation in national level and senior official exercises. DHS Directorates/Components conduct targeted exercises within their areas of particular responsibility. For example, the US Coast Guard recently conducted the California Spills of National Significance (SONS) exercise in April. These exercises are a component of the Coast Guard's National Preparedness for Response Exercise Program (PREP) to exercise and evaluate government Area Contingency Plans and industry spill response plans. OSLGCP and other components of DHS, as well as the interagency supported and participated in the exercise, which included significant private sector participation.

The creation of the Department of Homeland Security has greatly aided coordinating the inclusion of the private sector and critical infrastructure sectors in homeland security exercises by creating the Private Sector Office and the Information Analysis & Infrastructure Protection Directorate to ensure these partners are included in exercises. Past exercises, such as TOPOFF 2, have had extensive private sector participation.

Sharing exercise lessons and best practices.

A major goal of our National Exercise Program, development of a national system for collecting, reporting, analyzing, interpreting, and disseminating lessons and exemplary practices, was implemented on April 19th, 2004, when Secretary Ridge and Director Mencer announced the establishment of the Lessons Learned Information Sharing (LLIS.gov) system. Lessons Learned Information Sharing (LLIS.gov) is the national network of Lessons Learned and Best Practices for emergency response providers and homeland security officials. It was developed by the National Memorial Institute for the Prevention of Terrorism (MIPT), a non-profit institution established after the April 1995 bombing of the Murrah building in Oklahoma City. LLIS.gov is a secure system. All users are verified emergency response providers and homeland security officials at the local, state, and federal levels, and the system uses strong encryption and active site monitoring to protect all information housed on the system. Content is peer-validated by homeland security professionals for their peers. LLIS.gov also houses an extensive catalog of after-action reports (AARs) from exercises and actual incidents as well as an updated list of homeland security exercises, events and conferences.

The Department and its interagency counterparts routinely share lessons from sponsored exercises. These are done formally, within the Administration and during the course of concept development and planning conferences for other exercises. Unclassified lessons learned from other agencies' exercises are incorporated into the *Lessons Learned Information Sharing* system.Emergency response providers also set a LLIS research agenda and, whenever the priority research topics span other government agencies' areas of responsibility, the LLIS Team collects pertinent information to inform their research and analysis. As an example, published Best Practice series that incorporate lessons from HHS exercises include:

- Strategic National Stockpile Distribution
- Regional Emergency Planning for Healthcare Facilities
- Emergency Management Programs for Healthcare Facilities (to include emergency operations plans and hazard vulnerability analyses)

USNORTHCOM, through its Joint Interagency Coordination Group (JIACG), has provided its schedule of homeland defense and civil support exercises, which is posted on the Lessons Learned Information Sharing system and, through this site, shared with the emergency response community. The Lessons Learned Information Sharing research team is also working with the Interagency Homeland Air Security Steering Group co-chaired by DoD to capture and share lessons learned in the aviation security domain.

The current network of members stands at approximately 3,600 and is growing daily. The system is currently populated with hundreds of documents. Specifically, since its establishment on April 19, 2004, the site contains ten Best Practice series with a total of 87 documents, 57 Lessons Learned, and 20 Good Stories. To date the site includes almost 800 documents, 250 AARs, and hundreds of external links, news items, and event postings.

Learned and Good Stories are posted weekly. The original research agenda is continually being updated based upon input from the emergency response community. Lessons will be captured at all levels (state, local, and federal), and documents, events, and news items will be identified, formatted, and uploaded constantly. Lessons from DHS-sponsored exercises are captured in an after-action report analysis database. The tool is used to capture problems, positive performance, and lessons from DHS/OSLGCP-sponsored exercises by mission, discipline, and task.

Lessons from exercises are an important component in the development of state or urban area homeland security strategies, which are a key element in both the State Homeland Security and Urban Area Security Initiative Grant Programs. DHS/OSLGCP has worked with states and urban areas to establish exercise programs and multi-year exercise schedules, and requires submission of exercise after action reports. States are required to provide OSLGCP with copies of the AAR for all exercises conducted with OSLGCP funds. The AARs are analyzed by the Lessons Learned Information Sharing program to identify lessons learned and best practices that can be shared with other jurisdictions as well as to inform grant, exercise, and training programs.

To notify the first responder community of LLIS.gov's availability, both OSLGCP and the LLIS Team has embarked on an ambitious schedule to publicize this outstanding resource at numerous conferences, symposia, and events. OSLGCP is developing an Information Bulletin on Lessons Learned Information Sharing for release to the state and local homeland security community. In addition to public outreach events, other media have highlighted LLIS, including Aviation Week's Homeland Security & Defense (April 14); Federal Computer Week (19 April); ANSER Homeland Security Newsletter (25 June); Fire Chief Magazine (28 July); and the U.S. Conference of Mayors Newspaper (forthcoming). The website is accessible through the Department of Homeland Security Homepage; the National Governors Association; National Volunteer Fire Council; Association of State and Territorial Health Officials; U.S. Fire Administration; PoliceOne.com; Center for State Homeland Security; Public Health Foundation; and the International Association of Fire Chiefs.

Efforts to coordinate an effective cyber response capability across state and local jurisdictions and economic sectors and with the National Exercise Program (NEP) are underway in DHS' National Cyber Security Division.

Although the NEP is the responsibility of the Office of Domestic Preparedness (ODP), the NCSD retains overall responsibility for planning and execution of adequate cyber security exercises to measure and test readiness nationally. The NCSD now has a cyber security exercise program manager who works with ODP to schedule cyber-focused exercise elements in a manner that poses no undue burden on scarce resources including key personnel.

NCSD's involvement in the NEP is guided by two principles: (1) Cyber is only one element of a multifaceted NEP; cyber elements must be closely coordinated with other elements of that program to ensure efficient use of limited resources and the most effective return on exercise investments; (2) Cyber exercise elements must not be sidelined or relegated to an "afterthought" category within the NEP.

The federal government cannot by itself defend cyberspace from current or future threats. Acknowledging this, NCSD collaborates with industry and public-sector stakeholders across the country to define, develop, and exercise the major elements of a national cyber-space security response system. Its goals for the National Exercise Program (NEP) are to:

1. Sensitize a diverse constituency of private and public-sector decision-makers to a variety of potential cyber threats including strategic attack; .
2. Familiarize this constituency with DHS' concept of a national cyber response system and the importance of their role in it; and
3. Practice effective collaborative response to a variety of cyber attack scenarios, including crisis decision-making.
4. Provide an environment for evaluation of inter-agency and inter-sector business processes reliant on information infrastructure.
5. Measure the progress of ongoing u.S. efforts to defend against an attack.
6. Foster improved information sharing among government agencies and between government and industry.
7. Identify new technologies that could provide earlier warning of attacks.
8. Sort roles and responsibilities of government agencies and industry.
10. From the creation of the Department of Homeland Security you have quite appropriately described homeland security as a shared responsibility of the public and private sectors, especially since over 85 percent of the nation's critical infrastructure assets are owned and operated by the private sector. In a recent

speech commemorating the first anniversary of the Department it included a commitment to:

Work in greater tandem with the private sector to strengthen vertical communication systems and significantly increase permanent protections around our nation's most vital assets. The goal is to maximize real-time sharing of situational information without delay, and with full throttle distribution of intelligence to those in the field who need to act on it (presentation of Secretary Tom Ridge before the Homeland Security Policy Institute, George Washington University, February 23, 2004).

Could you describe in greater detail how you intend to accomplish this laudable goal and how you intend to include representatives of the private sector in the design and implementation of your plans? For example, are there any plans to integrate private sector experts into your analysis centers, either the HSOC or Cyber Watch Center?

Answer: In 2004, HSOC began the rollout of a national information sharing capability that is called the Homeland Security Information Network (HSIN). This network connects federal, state, local, tribal and private sector infrastructure stakeholders, enabling information sharing and collaboration within and among communities of interest. HSIN–CI (Critical Infrastructure) is a community of interest within HSIN that is dedicated to private sector components of the nation's critical infrastructure. A significant portion of the 2005 HSOC budget request is planned for growing the infrastructure and the reach of HSIN. HSOC is working closely with the Infrastructure Protection division of IAIP to identify and reach these private sector participants.

QUESTIONS FOR THE RECORD FROM THE HONORABLE SHEILA JACKSON-LEE

11. Given that the CIA's pre-existing Counter Terrorism Center works to fuse information analysis and operations with the input of several law enforcement agencies, why channel $865 million in fiscal year 2005 funds to the Terrorist Threat integration Center rather than channeling funds to the CIA's Center to make it better? Is it not possible to accomplish the same goals as with the TIIC with half the cost?

Answer: The National Counterterrorism Center (NCTC), formerly the Terrorist Threat Integration Center (TIIC), has not received and will not be receiving $865 million in fiscal year 2005 funds from either the Department of Homeland Security or any other element of the U.S. Government.

12. In this area, the Houston Task Force on Terrorism and its medical advisory steering committee are developing efforts to prepare for terrorist incidents and making sure that individual institutions have the information they need to be prepared.

The Houston public health and medical community is as well prepared as possible to detect and deal with infection by biological weapons. A tightly knit group of infectious disease specialists, strong city and county health departments and the communicable disease alert system (CDAS) help public officials maintain a close eye on the numbers and types of illnesses turning up in the area's clinics and emergency departments and to communicate this information to the public rapidly. This monitoring alerts them to patterns of disease that could be the result of bioterrorist activities. Because of refineries in Houston, chemical plants and other industries using dangerous materials, the city's health community is also well versed in treating individuals who have been exposed to life-threatening chemicals and in decontaminating patients as well as keeping health care facilities clear of such contamination. Already, education on the patterns of illness associated with bioterrorism or chemical terrorism is being distributed to physicians at the state and local level.

How does the Fiscal Year 2005 Budget propose to address the state-by-state disparities in the ability to prepare for bioterrorist attacks in hospitals and other medical facilities?

Answer: Under the Homeland Security Act of 2002 and Homeland Security Presidential Directive (HSPD)–7, the Department of Homeland Security (DHS) is responsible for leading, integrating, and coordinating implementation efforts among federal departments and agencies, state and local governments, and the private sector to protect United States critical infrastructure and key resources. HSPD–7 designates Sector-Specific Agencies responsible for infrastructure protection activities in a designated critical infrastructure sector, including conducting or facilitating vulnerability assessments and encouraging risk management strategies to protect against and mitigate the effects of attacks against critical infrastructure. The Department of Health and Human Services is the Sector-Specific Agency for the public health, healthcare and food (other than meat, poultry and egg products) sectors, and as

such would be responsible for collaborating with the aforementioned entities to encourage risk management strategies for hospitals and other medical facilities.

13. The need to fund improved threat assessment programs and to hire technical analysts to aid individual states and local areas can be found in Houston's drinking water vulnerability. Two-thirds of the drinking water provided to Houston residents comes from the San Jacinto and Trinity Rivers. These rivers are very vulnerable to pathogen and pesticide pollution, among other things. Houston's "Right-to-Know Report" earned a grade of "Poor" for 2000 and "Fair" for 2001. This report included a need for more prominent placement of the mandatory special alert for people who are more vulnerable to particular contaminants. The 2000 report provided a prominent and incorrect description of arsenic's health threat, and both reports offered misleading information about Cryptosporidium, which has been found in Houston's source water.

Our distinguished panelist indicates in his testimony that the President, in his Fiscal Year 2005 Budget, requests $11 million to fund a new biosurveillance initiative that purports to provide for "realtime integration of biosurveillance data. Will the IAIP suggest to the Department that part of these funds go to helping individual states to strengthen their threat assessment for bioterrorism?

Answer: As part of the larger Biosurveillance Initiative, the IAIP budget request of $11M is for the development of biosurveillance information integration capabilities that will provide improved early detection and characterization of bio-threats or developing disease events that may endanger our nation. Specifically, the National Bio-surveillance Integration System (NBIS) is an integrated geographic information assessment and response system for collecting, monitoring, and evaluating clinical and non-clinical biological threat information and reporting data streams from government and the private sector.

This NBIS system will leverage existing, emergent and future disease surveillance and detection systems, current Federal Department and agency capabilities, and other current state, industry and international disease surveillance and reporting capabilities. DHS has been working closely with Federal partners such as USDA, HHS, and EPA during the NBIS design phase—their existing biosurveillance capabilities are essential system components. DHS will continue to rely on those partners' subject matter and technical expertise and input throughout the development and implementation phases.

The $11M for biosurveillance also includes development of the National Bio-surveillance Integration Center (NBIC), which will facilitate real time analysis of disease and contamination events. The NBIC will provide National leadership with improved situational awareness of emergent biological events and will integrate various data streams from Federal partner agencies, States, and industry into a focused and refined status monitoring information stream.

Mature, integrated bio-surveillance systems will provide for the Federal and State Governments to effectively attribute bio-terrorism events and implement appropriate prevention, intervention and mitigation strategies, thereby enhancing the nation's ability to provide a coordinated, controlled, focused and measured national response to bio incidents.

Budgetary allotments for biosurveillance within IAIP will enable DHS to stand up NBIS functionality and establish the fusion capability for various bio-surveillance data streams. IAIP does not intend to use NBIS funding for bioterrorism assessments at the state level. Individual states have authority under the 2005 State Homeland Security Strategy Guidance to spend Fiscal Year 2005 Homeland Security Grant Program funds specifically for the purposes of bioterrorism threat assessments, if it fits into their homeland security strategy.

14. DHS Chemical Security Activities

In your testimony, you note that your Directorate has assisted in the conduct of vulnerability assessments and implementation of protective measures at many of the nation's highest risk chemical sites, thereby improving the safety of over 13 million Americans.

Secretary Libutti, can you tell me what exactly the Department has done to improve chemical security?

Answer: The Office of Infrastructure Protection (IP), part of the Information Analysis and Infrastructure Protection (IAIP) Directorate, uses a risk management process to develop and implement community-based security improvements around Critical Infrastructure and Key Resources (CI/KR) of greatest concern. IP maps threat information directly to identified vulnerabilities within and across sector segments. The process involves the identification of critical infrastructure and then the identi-

fication and assessment of vulnerabilities at those facilities and in the surrounding communities.

In the case of chemical sites, IP utilized the EPA RMP data as a starting point as part of a "worst-case" scenario modeling analysis to determine potential impacts of a terrorist attack. Using this conservative analysis, IP refined the methodology of the EPA consequence model, yielding results applicable to terrorist attack and not emergency preparedness. This led DHS to determine that there is only one chemical facility in the country that could impact over I million people, nearly 300 that could impact over 50,000 people, and roughly 3,800 facilities that could impact over 1,000 people. IP is concentrating efforts in fiscal year 2004 on those facilities that pose the greatest risk—the facilities that could potentially impact over 50,000 people.

Once these facilities are detected, vulnerabilities are then identified through Site Assistance Visits (SAVs). Over 30 SAVs have been conducted at chemical facilities so far this fiscal year to assist owners and local law enforcement officials in the identification of vulnerabilities and to facilitate mitigation option discussions. Owners and operators have independently implemented many of the protective measures identified in SAVs.

Using the information obtained during SAVs, as well as other sources of information, IP has also developed tools to bolster the physical security of chemical facilities. The first of these tools are Characteristic and Common Vulnerabilities (CCVs) reports. These CCVs concentrate on specific elements of critical infrastructure by providing specialized, sector-based information to help owners and operators bolster physical protection. By identifying common vulnerabilities in storage, refrigeration, or distribution related to the chemical industry, DHS can advise owners and operators how to better protect their facilities.

Further utilizing this sector-based approach, IP has also developed Potential Indicators of Terrorist Activity (PITAs) reports. PITAs call attention to terrorist surveillance, training, planning, preparation, or mobilization activities that may precede a terrorist attack, identifying both generic terrorist-related activates and those unique to each particular sector. The chemical sector PITA identifies potential surveillance techniques and local and regional indicators unique to the chemical sector that can alert facility operators to suspicious activities that may precede a terrorist attack.

Vulnerabilities are not only identified within chemical facilities; IP is facilitating the preparation and implementation of Buffer Zone Protection Plans (BZPP) within the chemical sector. The purpose of a BZPP is to identify protective measures around a specific facility that make it more difficult for terrorists to stage and launch a successful attack from the immediate vicinity of CI/KR. IP provides technical and material assistance to Local Law Enforcement (LLE) to mitigate vulnerabilities identified in the BZPP, effectively reducing vulnerabilities at the specific chemical site and building the general protection capacity of the community. Buffer zone plans provide scalable protective actions implemented in concert with changes in the Homeland Security Advisory System or as otherwise required, and are designed to provide an increased security posture.

Finally, to secure specific high-risk facilities better, a pilot Webcam program is being implemented at 13 high-risk chemical facilities. This equipment will help augment the overall security capability of these sites by providing 24-hour perimeter surveillance of established buffer zones. This information will be fed to LLE agencies and the Department, who will have the added capability of monitoring these sites continuously. All 13 high-risk chemical facilities are scheduled to have Webcam monitoring installed by September 30, 2004.

Last Tuesday, the President again called for the passage of comprehensive chemical security legislation. Can you tell us what that legislation will allow you to in terms of improving security that you cannot do now?

Answer: Regarding the Chemical Sector:

DHS continues to work with Congress on legislation to facilitate the protection of our Nation's chemical facilities, while considering the legitimate concerns of the private sector. However, we are not waiting for legislation. DHS has developed an effective working relationship with our private sector partners, and we are seeing good results and an increase in protection coming out of that developing partnership.

DHS has worked to accurately identify key assets, and to estimate their respective vulnerabilities.

- Using the EPA's Risk Management Program (RMP) database as a point of departure, DHS has estimated actual consequences of a successful attack on certain key assets. Our focus is on the potential impacts of terrorist attacks, so that protective actions can be prioritized at a Federal level. We have also done a basic evaluation of the chemical sector as a system (to the degree we have data available for such an assessment), so as to identify the most hazardous or

highest-risk sites, again to support prioritization at a Federal level, and also to support the decision-making processes of the State Homeland Security Advisors. This analysis included:

- Reviewing reported RMP status (materials held and quantities by vessel);
- Reviewing the population density in the vicinity of above-threshold (RMP) quantities of selected hazardous chemicals;
- Evaluating possible impacts of intentional attack instead of the accidental release model used in safety programs;
- Factoring RMP effected population estimates from a circle to a wedge, producing a rough estimate of actual, potential effected persons; and
- Modified plume modeling for more detailed effects prediction (where such modeling was deemed necessary to revise/validate estimates)

• To date, the Department's protective measures have been threat-based, focusing risk management efforts on the sites of greatest immediate concern. While the Department continues to work with our state, local and industry partners to refine the list of chemical sites, roughly 3,800 facilities that could impact over 1,000 people and nearly 300 facilities that could impact 50,000 or more people, and one facility that could impact over 1 million people have been identified. To date, DHS officials have visited more than 150 of the more than 300 chemical, petrochemical and related sites of greatest concern. The Department continues to visit these facilities on a priority basis.

• Going forward, these threat- based actions will be coupled with vulnerability reduction programs that will more systematically identify and develop best practices across the entire chemical sector, relating to the development and implementation of protective programs. Beyond the fence line of a specific plant, DHS continues its aggressive program to integrate community assets into the overall security posture of the chemical infrastructure. This effort includes both the Buffer Zone Protection Program, and a variety of educational, outreach, and coordination programs now in operation. The Chemical Sector-Specific Plan (an annex to the National Infrastructure Protection Plan that is scheduled to be available in December 2004) outlines many of these longer-term, more strategic initiatives.

Another major focus of the Department has been the development of guidelines, increased preparedness of law enforcement and first responders, and the implementation of protective measures at and around select chemical sites.

• Site visits are also conducted with chemical facilities as part of Buffer Zone Protection Plans (BZPPs). BZPPs are local efforts that contribute to reducing specific vulnerabilities by developing protective measures that extend from the critical infrastructure site to the surrounding community to deny terrorists an operational environment. The Department works in collaboration with state, local, and tribal entities by providing training workshops, seminars, technical assistance and a common template to standardize the BZPP development process. Local law enforcement takes a lead role in protecting its community as they are most familiar with the operational environment. To date, 65 plans developed by local law enforcement officials for chemical facilities have been submitted to the Department via State Homeland Security Advisors.

• As part of the protective buffer zone effort, web-based cameras are being installed at the 12 potentially highest-risk chemical facilities. The web cams will aid facility personnel and local law enforcement officials in detecting and deterring surveillance and other terrorist activities. Each site and local law enforcement officials will have access to the web cams.Additionally, the Homeland Security Operations Center (HSOC) at the Department's headquarters will also have access in order to create a real-time picture of the operating environment.

• The Department has also recently awarded five contracts for the development of next generation chemical sensors for both indoor and outdoor use. These sensors will be used in part to give immediate warning to areas surrounding chemical facilities in the event of an incident, whether intentional or accidental.

• All 2,040 member plants of the American Chemistry Council, as well as the entire membership of the Synthetic Organic Chemical Manufacturer's Association, and several other chemical industry trade associations, will have implemented strict voluntary security measures by the end of 2004. These Responsible Care companies have made great strides in improving security throughout the industry, and up and down the value chain. DHS continues to work closely with industry groups in order to develop security-oriented screening tools, assessment tools, best practices, and other processes to improve both our understanding of risk and vulnerability, and to improve our security on a site by site and infrastructure-wide basis.

DHS has also made major efforts in sharing information with law enforcement and the private sector.

• DHS is establishing or enhancing sector-specific information sharing and coordinating mechanisms for all of the 17 CI/KR sectors, incorporating both Information Sharing and Analysis Centers (ISACs) and Sector Coordinating Councils (SCCs). These entities have dual roles in that they serve as central points of infonnation sharing within each of the sectors and also act as the liaison to the federal government. Their main functions are to funnel threat information to facilities and receive and collect information from facilities. The Chemical Sector ISAC has supported Homeland Security's information sharing efforts since the Department's inception and includes over 600 individuals representing more than 430 different chemical companies.

• The Chemical Sector ISAC utilizes CHEMTREC, the chemical industry's 24-hour emergency communication center as the communication link between the Department and ISAC participants. When CHEMTREC receives information from DHS, that information is immediately transmitted, on an around-the-clock basis, to Chemical Sector ISAC participants utilizing electronic mail and a secure website.

• The Department introduced the Homeland Security Information Network (HSIN) on February 24, 2004, a real-time counter terrorism communications network currently connected to all 50 states, territories, and District of Columbia, as well as more than 50 major cities and urban areas. This program significantly strengthens the two-way flow of real-time threat information at the Sensitive-but-Unclassified level between the State, local, tribal, and private sector partners. By the end of this year, information at the SECRET level will be able to be shared with HSIN users.

• The Homeland Security Information Network initiative was expanded to include critical infrastructure owners and operators and the private sector in 13 states centered on the Dallas, Seattle, Indianapolis and Atlanta regions. The Homeland Security Information Network–Critical Infrastructure (HSIN–CI) Pilot Program is an unclassified network, which immediately provides the Department's Homeland Security Operations Center (HSOC) with one-stop, 24/7 access to a broad spectrum of industries, agencies and critical infrastructure across both the public and private sectors, including chemical facilities. This conduit for two-way information sharing provides the Department with an expanding base of locally knowledgeable experts and delivers real-time access to critical information. To date, HSIN–CI communicates with nearly 40,000 members.

The key to preparedness is educating law enforcement and private entities.

– Information derived from Site Assistance Visits (SAVs) are used to create two series of sector specific reports that are disseminated to owners, operators, security planners and local law enforcement officials to integrate into their respective risk management processes. The *Common Characteristics and Vulnerabilities* (CV) reports highlight common issues across chemical facilities so that relevant stakeholders can address possible vulnerabilities and improve overall site security. *Potential Indicators of Terrorist Attack* (PI) reports give further insight to owners, operators, and law enforcement official on how to better protect chemical facilities and, in turn, thousands of Americans in the surrounding communities.

• DHS has provided Buffer Zone Protection Plan workshops to state and local law enforcement officials in many cities who have chemical plants in their areas.

60 Minutes Report

Last November, the television program 60 Minutes reported it had examined security at 50 plants across the country and it had found widespread security gaps, including unlocked and open gates, dilapidated fences, absent guards, and easy access to containers storing tons of toxic chemicals.

Has DHS approached 60 Minutes to find out what they found and which plants had which deficiency?

Answer: DHS has not approached 60 Minutes to discuss their reporting on chemical plant security. While we work closely with the media in many areas, operational readiness is one which we treat seriously and do not want to create journalist conflicts.

Has DHS worked with any of these plants noted in this and other reports, such as

a. Neville Chemical Plant in Pittsburgh (33,000 people potentially effected)

b. The Univar plant in Forward, Pennsylvania (1.2 million people potentially effected)

c. Millenium Chemical Company in Baltimore (> 1 million people potentially effected)?

Answer: As described in QO1927, DHS utilizes a risk management process to map threat to vulnerabilities and uses a tiered approach to address facilities of greatest concern first. An assessment, including a Buffer Zone Protection Plan (BZPP), was conducted for the Neville Chemical Plant facility in conjunction with state and local law enforcement officials, security planners and the owners/operators. As the Sector Specific Agency (SSA) responsible for the chemical sector, DHS is developing a Sector Specific Plan (SSP) as part of the National Infrastructure Protection Plan (NIPP) in accordance with HSPD–7. The SSP for the chemical sector addresses the various types of facilities that could pose a threat to surrounding communities and builds on current activity being conducted by DHS to further protect chemical facilities.

15. Role of EPA

Reversing the principle outlined in National Strategy on Homeland Security, Homeland Security Presidential Directive-7 transferred responsibility for chemical plant security from the EPA to your Directorate at DHS. Last week, the White House reportedly forbade representatives from EPA from attending a hearing by the House Committee on Government Reform on the topic of chemical security. However, EPA already regulates the chemical industry for accidental, worker safety, and environmental protection issues.

Mr. Secretary, can you explain to us the logic behind removing EPA from the responsibility for chemical sector security?

Even though DHS has assumed responsibility for the chemical sector, the Department closely collaborates with the EPA in the protection of it. The close working relationship between the two agencies ensures that safety and security concerns are both addressed, taking advantage of both DHS and EPA's expertise in this area.

Are you working with EPA to can you assure us that facilities are not being overburdened by excessive or duplicative government interference or direction?

Answer: Yes. While DHS is tasked to secure these facilities, it must work closely with all other federal agencies to provide a strong security posture. For example, the Environment Protection Agency (EPA) has the mission to protect human health and the environment and to the degree it successfully monitors the safety and environmental compliance of these facilities, EPA contributes to the overall security posture of chemical facilities.

Furthermore, DHS and the EPA are working together on overarching national protection strategy documents, such as the forthcoming National Response Plan (NRP), which will serve as the primary document to guide domestic incident management, and the National Infrastructure Protection Plan (NIPP), which will provide a "roadmap" for protecting the nation's CI/KR and delineate roles and responsibilities to do so. This collaboration will continue to help ensure that our nation's chemical facilities are safe and secure without excessive government interference.

Synergistic Security Strategies

In considering a potential terrorist attack on a chemical facility, one should assume the intent of the attack is to cause a catastrophic release of toxic chemicals because this would pose the biggest risk to the public and is likely to cause the most fear. Given that avoiding the release of toxic chemicals is already the focus of most all accident, safety and environmental regulations, strategies, best practices, and technologies common to the industry, is DHS attempting at all to leverage these approaches to effect security improvements?

Answer: Yes. DHS seeks to bolster chemical facility security, not complicate it with unnecessary and time-consuming revisions. DHS' security and counterterrorism efforts that focus on protecting against malicious attacks are leveraged against EPA's ongoing efforts to prevent non-malicious accidents. Additionally, the private sector continues to develop and implement new technologies and best practices related to safety and security. The coordinated efforts of these three are required to best protect America.

QUESTIONS FOR THE RECORD FROM THE HON. JAMES R. LANGEVIN

As you know, much work has been done at the state level to identify and prioritize critical infrastructure, and I know that my state of Rhode Island has worked hard to develop such a list. I also know that at the federal level, a comprehensive and prioritized list of critical infrastructure is still lacking. It seems to

make sense that DHS should be taking advantage of the work already done by the states in this area.

16. Can you explain what information DHS has collected from states and the private sector regarding risk assessments and describe how it is being used by DHS to build a priority list? Is there a formal procedure for collecting and sharing this information, or is it a more informal or voluntarily process based on the initiative of individual states? If there is a formal process in place, who is responsible for collecting the information, how is it done, and how is it used?

Answer: The Department is encouraged by the progress states and the private sector has made in examining vulnerabilities in their communities. DHS utilizes a variety of informal avenues to collect information from the states and private sector entities as part of our national protective strategy. This includes tapping into the networks created by Information Sharing and Analysis Centers (ISACs) and relationships with private sector associations.

More formally, DHS collects vulnerability assessments and security plans via the US Coast Guard and Transportation Security Administration (TSA). Information is also collected in collaboration with local law enforcement officials and facility owners and operators through Site Assistance Visits (SAVs) and Buffer Zone Protection Plans (BZPPs). Another source of information is outreach conducted by sector specific agencies in accordance with HSPD–7.

Additionally, on July 19, 2004 states and localities were asked to participate in a data call intended to collect site information to further populate the National Asset Database (NADB), a growing registry of critical infrastructure and key resources (CI/KR). Information from all of these sources aids DHS to map threat information to vulnerabilities so protective programs can be prioritized.