PRIVATE SECTOR INFORMATION SHARING: WHAT IS IT, WHO DOES IT, AND WHAT'S WORKING AT DHS?

HEARING

BEFORE THE

SUBCOMMITTEE ON INTELLIGENCE, INFORMATION SHARING, AND TERRORISM RISK ASSESSMENT

OF THE

COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES

ONE HUNDRED TENTH CONGRESS

FIRST SESSION

JULY 26, 2007

Serial No. 110–62

Printed for the use of the Committee on Homeland Security

Available via the World Wide Web: http://www.gpoaccess.gov/congress/index.html

U.S. GOVERNMENT PRINTING OFFICE
48–957 PDF WASHINGTON : 2009

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON HOMELAND SECURITY

BENNIE G. THOMPSON, Mississippi, *Chairman*

LORETTA SANCHEZ, California,
EDWARD J. MARKEY, Massachusetts
NORMAN D. DICKS, Washington
JANE HARMAN, California
PETER A. DEFAZIO, Oregon
NITA M. LOWEY, New York
ELEANOR HOLMES NORTON, District of Columbia
ZOE LOFGREN, California
SHEILA JACKSON LEE, Texas
DONNA M. CHRISTENSEN, U.S. Virgin Islands
BOB ETHERIDGE, North Carolina
JAMES R. LANGEVIN, Rhode Island
HENRY CUELLAR, Texas
CHRISTOPHER P. CARNEY, Pennsylvania
YVETTE D. CLARKE, New York
AL GREEN, Texas
ED PERLMUTTER, Colorado

PETER T. KING, New York
LAMAR SMITH, Texas
CHRISTOPHER SHAYS, Connecticut
MARK E. SOUDER, Indiana
TOM DAVIS, Virginia
DANIEL E. LUNGREN, California
MIKE ROGERS, Alabama
BOBBY JINDAL, Louisiana
DAVID G. REICHERT, Washington
MICHAEL T. MCCAUL, Texas
CHARLES W. DENT, Pennsylvania
GINNY BROWN-WAITE, Florida
MARSHA BLACKBURN, Tennessee
GUS M. BILIRAKIS, Florida
DAVID DAVIS, Tennessee

JESSICA HERRERA-FLANIGAN, *Staff Director & General Counsel*
ROSALINE COHEN, *Chief Counsel*
MICHAEL TWINCHEK, *Chief Clerk*
ROBERT O'CONNOR, *Minority Staff Director*

SUBCOMMITTEE ON INTELLIGENCE, INFORMATION SHARING, AND TERRORISM RISK ASSESSMENT

JANE HARMAN, California, *Chair*

NORMAN D. DICKS, Washington
JAMES R. LANGEVIN, Rhode Island
CHRISTOPHER P. CARNEY, Pennsylvania
ED PERLMUTTER, Colorado
BENNIE G. THOMPSON, Mississippi *(Ex Officio)*

DAVID G. REICHERT, Washington
CHRISTOPHER SHAYS, Connecticut
CHARLES W. DENT, Pennsylvania
PETER T. KING, New York *(Ex Officio)*

THOMAS M. FINAN, *Director and Counsel*
BRANDON DECLET, *Counsel*
NATALIE NIXON, *Deputy Chief Clerk*
DERON MCELROY, *Minority Senior Professional Staff Member*

CONTENTS

PRIVATE SECTOR SHARING: WHAT IS IT, WHO DOES IT, AND WHAT'S WORKING AT DHS?

Thursday, July 26, 2007

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
SUBCOMMITTEE ON INTELLIGENCE, INFORMATION SHARING,
AND TERRORISM RISK ASSESSMENT,
Washington, DC.

The subcommittee met, pursuant to call, at 10:03 a.m., in Room 311, Cannon House Office Building, Hon. Jane Harman presiding.

Present: Representatives Harman, Dicks, Carney, Reichert, and Dent.

Ms. HARMAN. Good morning, everyone. We are pleased to be joined by our ranking member, Mr. Reichert, and our colleague, Mr. Dicks, and to welcome our panel and our second panel as well.

A few years ago the Homeland Security Department put out an endless, embarrassing list of critical national infrastructure that included everything from miniature golf courses to public swimming pools; in other words, a list that was almost useless to the private sector and to first responders.

Twoμdays ago the subcommittee had a Top Secret briefing on the Department of Homeland Security's Office of Infrastructure Protection Tier 1, Tier 2 program, and a list that once made people roll their eyes has been transformed. This is a good news story, and I congratulate the Department for getting its arms around what infrastructure is truly vulnerable and merits scarce Federal financial support.

Eighty-five percent of the Nation's critical infrastructure is owned by the private sector. It is not just the infrastructure, but most of the people of our country work in that infrastructure and most of the IT in our country is in that infrastructure. If we are to succeed in protecting that infrastructure and the people who work there, a better partnership between DHS and the private sector must be forged and it must work.

The news is not all good, and at this hearing we will hear from private sector firms about their inability, despite trying very hard to engage the Department and to work with the Department as a team. As any good business person knows, good customer service means giving customers what they want and need. Most importantly, the private sector needs to know how to prepare for and hopefully to prevent attacks against facilities, the personnel who work there and the surrounding communities. This is common sense.

What the subcommittee wants to know today is where the gaps are when it comes to this kind of private sector information sharing so we and the Department of Homeland Security can be effective in filling them. Here's the bottom line: If intelligence products don't tell businesses what actions to take in preparation for or in response to a threat, then it is not intelligence.

It is not as though the Department hasn't tried to be fair. In 2005, the Department's Private Sector Information Sharing Task Force issued a report that detailed how Homeland Security information should be shared with the private sector and recommended key steps to make it happen. But we are not clear how much progress has been made. In 2006, the Department's National Infrastructure Advisory Council issued a separate report on public-private intelligence coordination with its recommendations. We are not sure how that is going.

I am hoping our hearing today will shed some light on the status of these reports, but more important on how well the Department is implementing critical information sharing ideas with the private sector.

Our first panel of witnesses represents the key drivers of private sector information sharing at the Department. The Office of Intelligence and Analysis, the Infrastructure Protection and Preparedness Division and HITRAC.

I will ask, and I know all of our members want to hear, how each of your offices is doing to support private sector information sharing, how you are working together and where, if anywhere, there is duplication of effort. I also want to know how you are incorporating private sector input into the intelligence products you create, how successful those efforts are and what you are doing to improve on past performance.

We have found that with respect to intelligence generally, if you include the people who are going to use the information in the design of the information products, it becomes more useful. This, as they say in the intelligence business, is a "slam dunk."

Our second panel will be private sector witnesses, and I hope that they will be listening carefully to what the government witnesses have to say and offer constructive criticism.

The only way to ensure that relevant Homeland Security information is shared between the government and its customers, as I just said, whether they are law enforcement, first responder community or the private sector, is by working together to build a team. So I hope that after today our team will be stronger and all of you, next time you come back, will have good news to report.

Again, I congratulate the Department for the progress it is making, and I now yield to Ranking Member Reichert for his opening remarks.

Mr. REICHERT. Thank you, Madam Chair. Thank you for your leadership on this issue and for holding this important hearing.

And welcome to our witnesses this morning. Thank you for being here.

Our hearing today is about information sharing with the private sector, a critical component of our Federal government's information sharing efforts. As you know, the Seattle area is home to many

businesses that are critical to our Nation, include Boeing, Microsoft, Amazon.com and others.

While these and other private sector companies need information, we must also remember that information sharing is a two-way street. I believe that the Federal Government has a duty to provide situational awareness and share information on threats and vulnerabilities to representatives of the private sector. Likewise, the private sector has similar responsibility to provide information and to share with the Federal Government.

Oftentimes, the reason for not sharing is similar, the government or the company in question is concerned that a secret or a vulnerability will be revealed. The critical element to this relationship, I think we all recognize, is trust, specifically, cooperative partnerships that are based on trust. An essential element to building this trust is to protect the Critical Infrastructure Information Program, PCII. This program is designed to encourage private industry to share its sensitive, security-related business information by protecting information from public disclosure under the Freedom of Information Act, State and local disclosure laws and in civil litigation.

It is essential that PCII is successful. I believe it is important to ensure businesses have the proper incentives to share information and trust their Federal partners. I will be interested in hearing today how PCII is progressing and what may be done to improve participation. I would also like to hear what all of our witnesses have to say about the Homeland Security Information Network, specifically the HSIN critical sector portal.

I look forward to your testimony and very much appreciate your presence here today, taking the time out of your busy schedule to be part of this hearing. Thank you.

I yield.

Ms. HARMAN. I thank the ranking member and would point out that other members of the committee are permitted, under our rules, to submit statements, opening statements for the record.

Ms. HARMAN. It is now time to welcome our first panel.

Our first witness, Mr. James Chaparro, is the Deputy Assistant Secretary for Mission Integration in the Office of Intelligence and Analysis, that is, I&A, at the Department of Homeland Security. There is no possible way that fits on a business card.

He is responsible for the direction and oversight of I&A's program development and strategic planning efforts, as well as I&A liaison and information sharing activities within the U.S. and foreign intelligence communities; Federal, State and local law enforcement agencies; and other components of the U.S. Government. Mr. Chaparro serves as the Executive Director for the Homeland Security Intelligence Council, which was established to oversee and direct intelligence integration efforts within the Department.

Our second witness, Ms. Melissa Smislova, is the Director of the Homeland Infrastructure Threat and Risk Analysis Center, or HITRAC. HITRAC is a joint program office consisting of intelligence analysts from I&A and sector analysts from the Office of National Protection Programs Directorate and is charged with evaluating threats for homeland infrastructure.

And, again, I think the Tier 1–Tier 2 effort has come from the bottom of a deep hole into a very impressive place.

Our third witness, Mr. Jim Caverly, is the Director of the Infrastructure Partnerships Division, IPD, which resides within the Infrastructure Protection and Preparedness Directorate within the Department of Homeland Security. The Infrastructure Partnerships Division is responsible for sustaining core sector expertise, maintaining operational awareness and fostering working level relationships with industry, State and local government and Federal agencies representing vital infrastructure threats.

Without objection, your full statements will be inserted in the record. I would urge each of you to look at the little clock and to summarize your statement in 5 minutes or less; and we will then ask a round of questions before moving to our second panel.

Ms. HARMAN. We will start with Mr. Chaparro.

STATEMENT OF JAMES M. CHAPARRO, DEPUTY ASSISTANT SECRETARY, OFFICE OF INTELLIGENCE & ANALYSIS, U.S. DEPARTMENT OF HOMELAND SECURITY

Mr. CHAPARRO. Thank you, Chairman Harman and Ranking Member Reichert and distinguished members of the committee. I am pleased to have the opportunity to testify today about our information sharing efforts with the private sector.

I will start off by saying the men and women of DHS intelligence work day and night, weekends, holidays under very difficult circumstances to do the work that we do to protect the homeland, but we will not tire. We cannot rest and we cannot fail in what we do. Our mission is important and the threats are very real.

Just last week the Director of National Intelligence released a National Intelligence Assessment, or an NIE. An NIE, as you know, ma'am, offers a consolidated assessment of the Community and involves the work of the very best and brightest analytic minds that this country has to offer.

The threats to the homeland outlined in the NIE, I just want to talk about a couple of the key judgments very quickly.

Al-Qa'ida is and will remain a very serious threat to the homeland. Its central leadership continues to plot major plans or has plans for major plots against us. They will continue to intensify efforts to send operatives to the homeland, their plotting will likely continue to focus on prominent political, economic and infrastructure targets with a goal of producing mass casualties and visually dramatic destruction. They will continue to try to acquire chemical, biological and radiological capabilities, and they will not hesitate to use them.

It is DHS's shared responsibility to ensure the private sector has the intelligence it needs to better understand the threats that it faces and to understand their vulnerabilities and develop mitigation strategies to counter those threats.

We view the private sector as a vital partner in our efforts. I&A plays a critical role in providing threat intelligence to the owners and operators of our nation's infrastructure and key resources, or CI/KR, as it is commonly referred to.

In many ways, I&A's role within the National Intelligence Community is unique in the way it interfaces with the private sector.

VerDate Nov 24 2008 10:54 Aug 17, 2009 Jkt 000000 PO 00000 Frm 00008 Fmt 6633 Sfmt 6633 H:\DOCS\110-HRGS\110-62\48957.TXT HSEC PsN: DIANE

Our success in serving the private sector hinges upon our ability to share relevant, actionable and timely intelligence with the owners and operators of CI/KR. They deserve absolutely nothing less. We have statutory obligations and department-wide responsibilities for assessing and analyzing intelligence threats, and we recognize that the private sector needs to be a key part of our production cycle.

Close cooperation with the private sector allows us to help harvest key information that they see during their day-to-day interactions and also leveraging private sector information provides us a better understanding of their vulnerabilities and helps us fill critical intelligence gaps. We must, therefore, have a robust two-way flow of information.

We focus a great deal of energy in working with the private sector, both through our State and Local Fusion Center Program Office and through HITRAC which—I will not delve too much into HITRAC, because you are fortunate to have Ms. Smislova today.

Developing the actionable intelligence that the private sector needs is of little value if we cannot get that intelligence into the hands of the people who need it in a timely and efficient manner. So we have developed a very robust protection management division to disseminate our products and ensure that they wind up in the hands of the people who need to see them. This is a difficult task; the private sector is enormous and has many different sectors with many different needs.

We use comprehensive e-mail dissemination lists, we post products in a variety of formats, including classified-unclassified portals. And given the fact that posting an e-mailing product never does the job completely, we also make sure that we engage in extensive outreach with the private sector; and we are often out briefing our products through both the State and Local Fusion Center Program, as well HITRAC.

We are moving very rapidly with our fusion center program, thanks to great people in the support that we have received from this committee. We are rapidly expanding our deployment of officers to the field as well as our Homeland Secure Data Network, HSDN, and this is critical that we are able to interface at the local level with the private sector State and local law enforcement and State and local governments to be better able to carry out intelligence missions.

In summary, what I want to say, because I am running very short on time, is that the private sector needs context; they didn't need to hear spun-up threats that make them run off and expend resources on threats that are not credible. We try and add context to those threats and ensure that they receive the information that they need.

Thank you.

Ms. HARMAN. Thank you, right on time.

[The statement of Mr. Chapparo follows:]

PREPARED STATEMENT OF JAMES M. CHAPARRO

Thank you Chairwoman Harman, Ranking Member Reichert, and Members of the Sub Committee. I am pleased that you have provided me with the opportunity to appear before your Committee to discuss our role in sharing intelligence with the private sector, and to discuss the lessons we have learned.

The Office of Intelligence and Analysis (I&A) is transforming the way that DHS performs its intelligence responsibilities. As you know, I&A has established five overarching and bold priorities to carry out this transformation. Each of these focus areas are designed to allow us to provide our customers with the highest quality intelligence available, to protect the homeland, and to serve as good stewards of the resources that the Congress has provided us to carry out our mission. Our priorities are:

- mproving the quality and timeliness of intelligence analysis across the Department;
- Integrating DHS Intelligence across its several components;
- Strengthening our support to state, local, and tribal authorities, as well as to the private sector;
- Ensuring that DHS Intelligence takes its full place in the Intelligence Community; and,
- Solidifying our relationship with Congress by improving our transparency and responsiveness.

The Threats are Real and Our Work is Important:

Just last week, the Director of National Intelligence released a national intelligence estimate (NIE) that described the nature of the threat that we face in the Homeland. An NIE represents the Intelligence Community's most authoritative views on national security issues, is the product of extensive research and coordination, and involves the work of the best and brightest analytic minds that this country has to offer.

Among other things, the NIE assessed:

- Al-Qa'ida is and will remain the most serious terrorist threat to the Homeland, as its central leadership continues to plan high-impact plots, while pushing others in extremist Sunni communities to mimic its efforts and to supplement its capabilities;
- Al-Qa'ida will intensify its efforts to put operatives in the United States;
- Al-Qa'ida's Homeland plotting is likely to continue to focus on prominentpolitical, economic, and infrastructure targets with the goal of producing mass casualties, visually dramatic destruction, significant economic aftershocks, and/or fear among the US population.

I&A plays a critical role in providing vital intelligence to the owners and operators of our nation's critical infrastructure and key resources (CI/KR). In many respects, I&A's role is unique within the U.S. Intelligence Community (IC). We view our statutorily created partnerships with the private sector as critical to the success of I&A, and critical to the success of DHS.

I&A's success in serving the private sector hinges upon our ability to share actionable, timely and relevant intelligence. Our CI/KR owners and operators deserve nothing less. The Department of Homeland Security has been a leader in establishing new approaches of information sharing - including sharing with the private sector. To be fully effective in these approaches, we must partner not only with the private sector, but with other parts of the intelligence community such as the FBI, and with other agencies within DHS and the Federal government.

Because of I&A's unique capabilities and department-wide responsibilities for assessing and analyzing all terrorism, homeland security, and related law enforcement and intelligence information received by the Department, Secretary Chertoff has designated I&A as the Department's executive agent for information sharing. In this capacity, we have created many mechanisms to bring together DHS' vast knowledge base and expertise to strengthen information sharing across the Department and, even more importantly, to share it with our external partners.

I would like to impart upon you today some of the information sharing efforts that DHS is leading, as well as describing some of our efforts with our Federal and intelligence community partners. The central theme you will see throughout is that we view the private sector as a vital partner in our efforts, just as we view the FBI, and our state and local government partners.

As I noted above, the NIE assesses that Al-Qa'ida's focus includes economic and infrastructure targets. A large number of these potential targets are owned and/or operated by our private sector partners. It is our shared goal—our shared *responsibility*—to ensure that the private sector has the intelligence it needs to better understand the threats they face, as well as the vulnerabilities that can be exploited by our enemies. The private sector is more than just a customer of our intelligence products; they are a critical part of our production cycle. Given the size, diversity and complexity of the private sector, close cooperation with them is key to helping us understand the threats and vulnerabilities that exist. The private sector provides us with windows into understanding the threat based on their day-to-day observa-

tions and interactions across the country, helps us better understand their intelligence needs, and provides us with unique perspectives that help us fill intelligence gaps. We must therefore ensure a robust two-way flow of information between the Department and our private sector partners, as well as between our federal, state, local and tribal partners

Strengthening the Flow of Intelligence

DHS has focused a great deal of energy to ensure that our private sector partners receive the very best intelligence available. A linchpin of this effort is the Homeland Intelligence and Threat Analysis Center (HITRAC), a three-way partnership between our Office of Infrastructure Protection, I&A and the Private Sector. I will not delve deeply into how HITRAC functions, because we are fortunate that Ms. Smislova, HITRAC's Director, is here to testify today. What I will say, however, is that HITRAC produces a variety of classified and unclassified intelligence products specifically tailored to serve private sector intelligence needs which is a unique effort within the Federal government. In addition to working with the DHS Office of Infrastructure Protection and its private sector partners, HITRAC closely coordinates its efforts with agencies such as the FBI, Transportation Security Administration, and the National Counter Terrorism Center.

Good intelligence is of little value unless it can be put into the hands of those who need it. I&A has established a strong Production Management (PM) division to ensure that our intelligence products, including those produced by HITRAC, are disseminated in a timely and efficient manner. Just as HITRAC's customers are diverse, so too must be our intelligence dissemination methods.

The I&A PM Division maintains comprehensive email dissemination lists, specifically designed to serve private sector partners at the unclassified level. Email distribution occurs using the Sector Coordinating Councils (SCCs), and when appropriate, Information Sharing and Analysis Centers (ISACs) list points of contact across the 17 CI/KR sectors : Chemical, Commercial Facilities, Dams, Emergency Services, Energy, Banking and Finance Agriculture and Food, Government Facilities, Public Health and Healthcare, National Monuments and Icons, Information Technology, Commercial Nuclear Reactors, Materials and Waste , Postal & Shipping, Telecommunications, Defense Industrial Base, Drinking Water and Water Treatment Facilities, and Transportation (including Aviation, Maritime, Railroad, Mass Transit, Highway),. In addition to the email to the SCCs and ISACs, products are sent to the DHS National Infrastructure Coordinating Center (NICC) for posting to the corresponding unclassified HSIN—Critical Sectors where more private sector partners can view the products. Similarly, products classified at the Secret level are posted on the Homeland Secure Data Network (HSDN)—a network that is rapidly expanding, thanks in part to our efforts in the State and Local Fusion Center (SLFC) program.

However, sending emails and posting products is not enough. I&A's analysts also engage in extensive outreach efforts directly with private sector representatives, through HITRAC and the State and Local relationships. This effort generally is initiated by the State or locality itself and, is designed to push and pull information that directly relates to threats within a particular geographic region where, for example, that individual sector may be headquartered or maintain critical assets, such as plants or distribution centers. The response has been positive.

Moreover, state and local fusion centers (SLFCs) are increasingly helping to bridge the gap between sector specific threats and geographic threats, by such efforts as involving plant managers and small businesses - not just corporate offices—in fusion center activities. The private sector wants relationships built on trust. I&A is taking full advantage of the fact that many SLFC officials have already built strong private sector ties in their communities.

An example of this local dynamic is in Illinois, where the State Terrorism Intelligence Center (STIC) is using their State HSIN Portal as the primary tool for information sharing with the Private Sector. Major companies like Caterpillar, McDonald's, Cargill, and John Deere are part of this process, as well as smaller businesses that were identified through State incorporation listings.

Maryland is another fine example. Maryland has formed a Private Sector Council that has leaders from a number of Maryland based companies—big and small—who advise the Maryland Coordination and Analysis Center (MCAC), Maryland's primary fusion center, routinely on their information needs. Maryland's Private Sector Council has been formally recognized by the MCAC and they meet monthly to discuss threat-related issues within Maryland and the National Capital Region. While the main conduit in these examples is through the State Fusion Centers, both involve support from and frequent interaction with DHS.

The private sector needs a comprehensive understanding of the threats they face in order to develop mitigation strategies, to plan for continuity of operations in the event of an attack or disaster, and to protect its employees and assets. In addition to understanding credible threats, the private sector also needs to be aware of threats that lack credibility. I&A helps to add context to raw intelligence reporting to help the private sector better understand which threats are real and which ones don't necessarily require a response. This helps the private sector better manage its resources.

Write to Release—But Protect Privacy

DHS is participating in many federal efforts to further improve information sharing with the private sector. At the national level—DHS in conjunction with DOJ and the DNI, is creating the Interagency Threat Assessment and Coordination Group (ITACG). The ITACG is being established in response to the President's Guidelines for the creation and establishment of the Information Sharing Environment. The group will be part of the National Counterterrorism Center (NCTC) and will enable the development of intelligence reports on terrorist threats threat and related issues that represent a federally coordinated perspective and are tailored to meet the needs of state, local, and tribal governments. The ITAGC will be staffed by DHS and FBI personnel and will include representation from state and local entities. The coordination of counterterrorism information within NCTC ensures that products released from the Federal government will be of one voice and without delay. By including State and local partners as members of the ITAGC, the language appearing in federally disseminated products can be more focused or tailored in areas that are of greater interest and in a form that is most useful non-federal partners.

Similarly, there are many indisputably legitimate reasons for protecting sensitive information—even information that is unclassified. For example, information which we refer to generically as Sensitive but Unclassified (SBU) or Controlled Unclassified Information (CUI). Examples of CUI include personal information, information that could compromise ongoing law enforcement investigations or endanger witnesses, information containing private sector proprietary information, and information containing private sector vulnerabilities and other security-related information that could be exploited by terrorists. Inappropriate disclosure of these types of information could cause injury to individuals, business, or government interests. We must balance the need to produce actionable intelligence, while protecting the liberties and rights of both individuals and businesses.

DHS understands the importance of protecting private sector proprietary information. We have created handling controls to facilitate information sharing in a protected manner. Within DHS, there are three such information-protection regimes—"Protected Critical Infrastructure Information (PCII)," "Sensitive Security Information (SSI)," and the newly established "Chemical Vulnerability Information (CVI)."Congress mandated these categories of information be protected and DHS has promulgated regulations implementing these regimes. Each was specifically created to foster private sector confidence to increase their willingness to share with the federal government crucial homeland security-related information. To date, PCII and SSI have been successful in this regard and have been well-received by the private sector. Moreover, these designations are ready examples of how robust control of information can actually promote appropriate sharing.

Additionally, DHS is working with the Program Manager of the Information Sharing Environment (PM–ISE) and key information sharing stakeholders on the SBU Coordinating Committee to implement the President's direction in Presidential Guideline 3, which, among other things, directs departments and agencies to provide recommendations to standardize sensitive but unclassified information handling and marking procedures so that federal agencies can more efficiently and effectively share SBU information with its many partners.

Conclusion

I appreciate the opportunity to share with you our efforts of sharing intelligence with the private sector. DHS recognizes the private sector not only as a critical customer, but a vital partner in protecting the homeland. I&A is dedicated to strengthening the information flow with our infrastructure threat analysis and the extensive distribution of theses products. DHS believes the private sector is an important part of our nation's intelligence cycle and actively engages them to help us understand real time requirements. We are building excellent private sector relationships through our State and local Fusion Centers. DHS is actively and collaboratively working with our Federal partners including DNI, FBI and others to ensure that the private sector can obtain the best available intelligence in a timely manner. We are dedicated to this important relationship and will continue to work to find new ways of strengthening it in support of homeland security.

Ms. HARMAN. Ms. Smislova, you are now recognized to summarize your statement in 5 minutes.

STATEMENT OF MELISSA SMISLOVA, DIRECTOR, HOMELAND INFRASTRUCTURE THREAT & RISK ANALYSIS CENTER, DEPARTMENT OF HOMELAND SECURITY

Ms. SMISLOVA. Thank you, ma'am. Good morning, Chairwoman Harman, Ranking Member Reichert and other members of this subcommittee.

I am very happy to have this opportunity to talk with you about the progress that the Department has made and, in particular, HITRAC has made in sharing information with the private sector.

I did, in fact, testify before this same subcommittee in Novemberμ2005. At that time, HITRAC, the Homeland Infrastructure Threat and Risk Analysis Structure, was only 8μmonths old, and so much of my testimony discussed what we had hoped to do, what our plans were, the initial outreach we had made to the private sector.

Since Novemberμ2005, we have produced over 171 products that were aimed specifically for the private sector. In addition, we have conducted hundreds of threat briefings to different members of the private sector.

Having said that, we do know that there is much that remains to be done; and we have learned quite a bit about our customer, we have learned much about what works and we have learned some about what doesn't work.

First, though, I wanted to give you a brief update on where HITRAC is. Again, when I testified in November 2005, there were different changes in the Department of Homeland Security, and we have had an exciting several years.

I am the Director of HITRAC, and I am an intelligence professional. I work for Mary Connell and Charlie Allen. My deputy, Brandon Wales, did brief you Tuesday evening on the Tier 1-Tier 2 program, and he is an infrastructure protection employee. We are a joint program office that is staffed by intelligence professionals, such as myself, and then nonintelligence professionals that have more insight into infrastructure requirements—security, as well as what the infrastructure looks like and what they may need to make informed decisions.

I also am the Director of the Critical Infrastructure Threat Analysis Division. I only bring this up to underscore that intelligence information produced by the Department of Homeland Security all does go through the appropriate intelligence chain of command. So all of the intelligence information that HITRAC does send out is approved by Charlie Allen so as to ensure that the intelligence is valid and vetted.

I wanted to talk first, briefly, about the kinds of products that we have learned work with the private sector. We started with a strategic sector assessment, and those are the products I discussed in my November 2005 testimony. They were intended to be baselines: What does the terrorist information say about their interest in attacking specific sectors, so that we would bring the private sector up to date on all the specific information that we had.

In addition, we attempted to provide a portrait of this adversary to say what we believe the attack methods might be and what goals he might want to achieve, trying to provide the private sector with a better sense of whether or not they should protect against one specific attack over another.

I am not sure who benefited more from the strategic sector assessments, us in dealing with the private sector and learning more about the United States railroad system or the oil and gas industry or the private sector. But we did accomplish that mission, and we did provide sector assessments for all of the critical infrastructure sectors as defined in HSPD–7.

Our other products that have, I think, proven just as useful—and maybe in the future, even more—include infrastructure intelligence notes. They summarize events overseas, such as the chlorine-boosted VBIEDs; they discuss other tactics and other techniques that we are gleaning from terrorist activities overseas; and we update the private sector on items of interest, such as the London attempted bombing.

We also help Mr. Allen with the CINT notes that go out and provide the private sector with specific immediate information about activities.

In addition, we provide a great deal of threat briefings and outreach to the private sector. This proves to be one of our larger challenges. As you mentioned, Chairman Harman, 85 percent of the infrastructure is privately owned; and this is a large country, so that part has proven to be very, very challenging. People like to have a personal briefing, and we do that in conjunction with Mr. Caverly's infrastructure protection plan partnership model that has assisted us greatly.

So, in closing, I think some of our challenges include educating the private sector on what we can and can't provide. They also include the outreach, trying to get everyone included in our outreach, as opposed to some people; and that part remains a challenge. Dissemination of our products is also a problem, again, given the size of the audience.

But I am happy to report we have made significant progress, and I look forward to briefing you on successes in the future. Thank you.

Ms. HARMAN. Thank you very much.

[The statement of Ms. Smislova follows:]

PREPARED STATEMENT OF MELISSA SMISLOVA

Introduction

Good morning, Chairwoman Harman, Ranking member Reichert, and distinguished Members of this Subcommittee. I welcome the opportunity to speak again to this subcommittee on the progress of the Department of Homeland Security in sharing intelligence information with the private sector. I will also take this time to discuss the lessons we have learned during our outreach and inform you of our plans to improve information sharing.

I manage both the Department's joint program office for assessing the risk to the critical infrastructure and key resources of the United States, known as the Homeland Infrastructure Threat and Risk Analysis Center (HITRAC), as well as the DHS Office of Intelligence and Analysis (I&A), Critical Infrastructure Threat Analysis Division (CITA), which supports HITRAC as its discrete, embedded intelligence component. Through my involvement with HITRAC and CITA, I am able to oversee the collocation of DHS intelligence analysts with the Department's infrastructure protection experts responsible for performing sector-specific risk assessments. The vir-

tue of maintaining CITA's existence as a separate albeit embedded threat unit within HITRAC ensures that all intelligence production remains subject to the oversight and policies of the Department's Assistant Secretary for Intelligence and Analysis and Chief Intelligence Officer.

Production

Since I last testified to this subcommittee in November 2005 significant progress has been made in developing and disseminating products and briefings tailored specifically for the private sector audience. In that time, HITRAC/CITA has produced over 171 separate products for critical infrastructure protection analysts in the private sector, State and local homeland security agencies, and the law enforcement community. Of these, 40 were assessments jointly written and published with the Counter Terrorism Division of the Federal Bureau of Investigation.

We have also systematically and routinely conducted classified and unclassified intelligence briefings for the private sector, largely through the National Infrastructure Protection Plan Partnership Model, but also through our discrete relationships with industry associations, our attendance at conferences, and outreach directly to individual private sector entities.

While I am proud of our accomplishments and I believe the work done so far creates a good baseline, I do know that much work remains. As our relationship grows with the private sector and with the critical infrastructure community in State and local governments, we are increasingly learning about new requirements. The information needs of the private sector and of the States are diverse, and we are challenged to create products and briefings to meet them.

One of the first lessons we learned was that private sector and the critical infrastructure protection officials in State and local law enforcement community's work closely together yet sometimes have different information requirements. We began our HITRAC/CITA production efforts with assessments aimed at addressing known and potential threats to sectors—or systems—of like critical infrastructure. While we found that those products were well received by some our private sector customers, States were more interested in regionally focused analyses. We have responded by expanding our product lines and outreach efforts to address, in addition to core sector specific concerns, the broader, cross-sector regional issues.

Intelligence Information Designed for the Private Sector

We produce classified assessments and do regularly give classified briefings to members of the private sector. The Department of Homeland Security and FBI have sponsored many of our customers for clearances to receive classified information. We also disseminate these assessments at various classification levels, modified, of course, to adhere to all applicable classification rules and other requirements for protecting sensitive information, but with the goal of reaching as many customers as possible.

However, our interaction with the private sector has underscored their interest in the details of intelligence reports vice source information. Much of what makes a report classified is its reference to collection. Because of that focus we have been very successful in working with the intelligence community to ensure the downgrading of key information on terrorist tactics, techniques and procedures. Many of our products use information we have first worked to downgrade from classified to unclassified.

Another lesson learned was that many within the critical infrastructure information sharing community were interested in reporting about numerous sectors. Thus, we expanded dissemination.

Our product lines now respond to what we have gathered about private sector needs and continue to evolve with private sector involvement. We continually reach out to a broad spectrum of private sector representatives to refine the scope of our assessments, and have come to learn that private sector information requirements are not only numerous, but have become more complex as our private sector partners have become more knowledgeable about intelligence and terrorism generally. Thus, where in the beginning many of our products summarized merely what was known about existing terrorists' interest in certain types of infrastructure as potential targets, our product lines now reflect our customers expanded interests in more detailed analysis of terrorist tradecraft, including especially surveillance techniques and attack methods.

Many of our products have benefited from the insight and, in many cases, direct input of members of the private sector as those products are being developed. In addition, this direct interaction with the private sector has also assisted the Department in clarifying, or putting into better context, vague or incomplete threat reporting.

Some of our current product lines include:

• ***Quarterly and Annual Suspicious Activity Assessment (SAA):*** These assessments provide strategic, national-level analysis of suspicious incidents reported to DHS. They use information provided by the private sector and are an attempt to provide industry with trend and pattern analysis of incidents noted at their facilities. This represents a genuine and valued partnership between the government and private industry.

With the direct involvement and knowledgeable support of the private sector, we have been able to establish a baseline of "suspicious activity" reflected in these assessments. For example, when we recently received reports that electrical power towers were possibly being sabotaged, private sector electrical industry professional familiar with that particular region suggested to us that the activity was more likely illegal, albeit non terrorist related, tampering often seen in that area of the country during hunting season—i.e., elements of the power towers are used illegally to create deer blinds. Similarly, we believe we have been able to better educate the private sector about terrorist surveillance techniques and alert them when suspicious activity might indicate pre-operational terrorist activity.

• **CINT Notes—**In conjunction with notes regularly sent out by the Chief Intelligence Officer, Charlie Allen, concerning current threat activities or information, we communicate directly with all stake-holders, including the private sector, to inform them of what we know about incidents as they unfold. CINT notes and follow up coordination with relevant partners concerning the recent attempted attacks in London and Glasgow is a good example of this means for sharing pertinent information.

Mr. Allen also makes direct phone calls to US companies if they are specifically mentioned in intelligence reporting.

• ***Infrastructure Intelligence Note (IIN)***—Generally a short product that provides the infrastructure owners and operators and State and local partners with a timely perspective on events, activities, or information of importance to support security planning. These products differ from the CINT notes in that they entail more research and time to craft. Some Infrastructure Intelligence Notes are generated directly by calls from private industry based upon specific sector questions or concerns. We also use the Infrastructure Intelligence Note to discuss lessons learned from terrorists' attacks overseas. These assessments are provided to enhance our critical infrastructure protection community's understanding of evolving terrorist tactics, techniques, and procedures.

• ***Joint Homeland Security Assessment***—Products written with the Counter Terrorism Division of the Federal Bureau of Investigation. These assessments communicate intelligence information that affects the security of U.S. citizens or infrastructure. Provides information on training, tactics, or terrorist strategies, and analyzes incident trends and patterns. This product also may recommend protective measures. During the last two years we have built a valued and productive relationship with our colleagues at the FBI. This partnership not only produced more comprehensive assessments, but ensures that the government speaks with one voice to our customers. * Strategic Sector Assessments—These were our first unique HITRAC products and were intended to provide a baseline analysis of the threats and risks to the entire critical infrastructure. These products are written at multiple classification levels, detail our analysis of the intentions and capabilities of known terrorists, and integrate relevant threat information. Some of the sector-specific assessments include discussion of the unique vulnerabilities and consequences unique to that sector.

• ***State and Regional Threat Assessments***—As I mentioned, one of our lessons learned is that elements of the critical infrastructure community are interested in regionally focused assessments. This is an area of production we are working on with the support of private sector and State partners. While we have created several regional assessments, our efforts are in the beginning stages.

Lessons Learned and Future Opportunities

We continue to modify our processes and products based on customer feedback and other lessons learned. We believe these modifications have made us more responsive to our stakeholders and have enabled us to create better products.

Integration with State and Local governments.

While our initial efforts were focused on the CI/KR owners and operators, we have dramatically increased our work for and with State and local authorities who have significant responsibilities for security, risk mitigation and incident response around the nation CI/KR.

We now have an aggressive outreach plan that includes State and local as well as private sector critical partners to identify information needs and to tailor analyses and products to meet these requirements. As part of this outreach plan, we are regularly meeting with Homeland Security Advisors and their staffs to integrate State information and their analysis into the creation of state critical infrastructure threat assessments. By doing this we hope to gain a more comprehensive appreciation for the threats in the states.

Specific Outreach initiatives. We initiated and continue to participate in weekly conference calls with multiple critical infrastructure sectors as well as an analytic exchange between DHS intelligence analysts and State and Local Fusion Centers.

Conclusion

In conclusion, I believe partnering intelligence professionals with sector experts and security personnel has proven successful for developing better threat assessments. I believe we have made significant progress developing product lines and briefings that provide tailored intelligence information to the private sector, States and law enforcement communities.

We are excited about improving our analytic understandings of the various threats to critical infrastructure. We understand that working in partnership with the private sector, States, and local governments is the way to achieve that improvement. Our goals for the future include enhancing our regionally focused assessments and better integrating vulnerability and consequence data into our analysis.

Thank you.

Ms. HARMAN. Now, Mr. Caverly, you are recognized for 5 minutes.

STATEMENT OF R. JAMES CAVERLY, DIRECTOR, PARTNERSHIPS AND OUTREACH DIVISION, OFFICE OF INFRASTRUCTURE PROTECTION, DHS

Mr. CAVERLY. Thank you, Madame Chairman, Ranking Member Reichert and members of the subcommittee. It is a pleasure to be here today to talk about the framework and the structure that we have put in place to be able to share information with the private sector and to allow them to share information with us.

Building trust in an effective working relationship is critical to being able to share that information. It is not only about being able to get the information out there, but the ability to have the trust that is necessary.

I believe the subcommittee is well aware, in the National Infrastructure Protection Plan we have defined a very good structure for sector partnership and also for information sharing. And we have taken that forward from the development process and implemented as fully as I believe we can at this stage.

Sharing information with 17 different sectors is difficult because each of the sectors is different, and we have to tailor the structure of the mechanisms and, ultimately, the product to each sector, because talking to a nuclear power plant is different than talking to a railroad.

We know information sharing has to be two ways. We know that between government and the private sector we need to share information on trends of threat, criticality, the consequences of things, the vulnerabilities based on those emerging threats, protection priorities and best practices. That sharing back and forth is what enhances both what the government needs to do to protect critical infrastructure and what the owners and operators need to do.

That information has to inform things at three levels:

We have to be able to give them strategic information that informs their investments in their planning and structures with the long lead times;

We have to be able to give them situational assessments that let them know what is going on right now; and

The third piece is, we have to be able to provide them the tactical level of information that says to a security director, based on what you told me, I either do or don't need to do something differently.

We have some challenges in that. We have the challenges of classification information, we have the challenges of ways to communicate to get directly to those owners and operators. We think we have put some of those in place.

As I mentioned, our sector partnership model with a sector coordinating council gives us the ability to shape our products and structures in a way that is relevant to each of the infrastructure sectors. We also know, through our CIPAC activity, our Critical Infrastructure Partnership Advisory Council, using the authorities Congress gave us in 871, we have been able to create an environment in which we can share the sensitive information without the risk of its being disclosed inadvertently to places it shouldn't go. I believe everybody agrees that vulnerability data is not well served by being in the public domain,

Chairwoman, as you mentioned, the National Infrastructure Advisory Committee did a very good study on information sharing. A range of those recommendations have been implemented. I understand there was testimony yesterday to another subcommittee from a member of the advisory committee of NIAC who, in fact, complimented the implementation of the recommendation.

We set in place a couple of things that are quite important to understand. We put the National Infrastructure Coordinating Center in, which is a 7-by-24 operation, a hub for our interaction and communications with the private sector. It is part of the National Operations Center. Its job is to provide the always-there connectivity to the private sector. All of our information goes out through it, and it provides them the ability to reach in and connect with us any time from any place.

You mentioned the Homeland Security Information Critical Sector. It is a critical system for us because we believe that there has to be the capability of a common platform that serves not only the individual sectors, but also the cross sectors. It is equally important; I think it is the government's function to provide that platform. The reason is, if we ask the private sector to provide it, there would be barriers to participation from those companies and small entities that don't have the resources to participate. So we have gone down the path of building a structured mechanism that will serve all the members of the sector and have barrier-free access.

You mentioned the Protected Critical Infrastructure Information Program. As you are aware, this past spring we issued the final regulations. We now have over 5,000 different elements of information that have submitted under the PCII program. We believe that as the private sector gains the government's ability to protect that information and not have it disclosed inadvertently, we will have more participation in the program.

We have to be able to convince the private sector that, A, we need the information and tell them why and what will happen with it and then make sure that we carry through on that. So we think that is a program that will grow totally on trust.

The last thing I would like to mention briefly is, we have embarked on a program from the beginning of providing clearances to members of the private sector. We are expanding that. We have over 1,000 members now that have the clearance, but that is essential to being able to share sensitive information with the people who have to be able to do the decision-making, so that is an important part of our activities.

The last thing, there is a major initiative under the Intelligence Reorganization Act for the information sharing environment, of which we are a major component of that. And, in fact, in dealing with the sharing of information in private sector out of the DNI's office and the program manager's office, they have taken our structure in the NICC for the Sector Coordinating Councils and the private sector relationship to be the basis on which they are exploring that issue.

Thank you.

[The statement of Mr. Caverly follows:]

PREPARED STATEMENT R. JAMES CAVERLY

Thank you Chairwoman Harman, Ranking Member Reichert, and Members of the Subcommittee. It is a pleasure to appear before you today to discuss the Department of Homeland Security's (DHS's) perspective on private-sector information sharing, specifically with the nation's Critical Infrastructure and Key Resources (CI/KR) stakeholders.

The challenge of protecting the nation's CI/KR is daunting. Human, physical, and cyber assets, systems, networks, and functions are spread across 17 critical infrastructure and key resource sectors, diverse in their composition, cultures, regulatory regimes, and operational processes. In aggregate, the CI/KR sectors represent almost 50 percent of the nation's Gross Domestic Product, with a majority of assets, systems, and networks owned and operated by the private sector. The protection of the nation's CI/KR represents a shared responsibility by owners, operators, and all levels of government through complementary commitment of resources, knowledge, and capabilities.

Building trust and effective working relationships with the private sector to facilitate information sharing is essential for effective CI/KR protection. The Sector Partnership model and other information-sharing mechanisms and tools described in the National Infrastructure Protection Plan (NIPP) provide the structure and processes within which public- and private-sector security partners share vital information to mitigate the nation's CI/KR risks.

The Challenge of Information Sharing

The NIPP defines the nation's CI/KR as "those systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."

The wide scope of this definition of CI/KR underscores the wide variety in the 17 sectors' approaches to information sharing. Sectors differ in business characteristics and their sensitivity to risk taking; the assets, systems, networks, and functions involved; their previous experience in working with government; and the specific risk-management characteristics of the sector.

One factor that all CI/KR sectors have in common, however, is that in their public-private partnerships necessary for CI/KR protection, the desired outcome is a safer, more secure, and more resilient sector. Information sharing is effective when it clearly and directly supports this outcome.

Because information sharing is valued by both the CI/KR owners and operators and by the government, a collaborative approach enables public and private security partners to determine how best to apply their respective resources and capabilities to the entire spectrum of risk-management activities: prevention/?deterrence; protective programs; preparedness; response and crisis management; and, recovery, restoration, and reconstitution.

Information Sharing and CI/KR Decision Making

Information sharing by both public- and private-sector security partners on threat trends, criticality (consequences), possible vulnerabilities based on emerging threats, protective priorities, best practices, and strategic solutions enables CI/KR risk management and must support several levels of decision making:

(1) Strategic planning and investments in preparedness and protective programs by both CI/KR owners and operators and government at all levels.

(2) Situational awareness and decision-making coordination during the execution of planned preparatory actions, protective measures, and response/recovery efforts.

(3) Operational/tactical decision making through the exchange of incident or suspicious activities information and the timely and accurate transmission of alerts and threats to CI/KR owners and operators to catalyze protective actions.

In the complex, dynamic environment that is characteristic of CI/KR-protection decision making, effective information sharing must be centered on clearly defined "knowledge networks" of public- and private-sector professionals and senior managers with the ability and authority to make decisions and act on critical, focused information. The bottom line for CI/KR information sharing is to get the right information to the right people who can make decisions and take the correct actions to protect the CI/KR and to mitigate consequences.

The Sector Partnership

The Sector Partnership model described in the NIPP is the foundation for effective information sharing with the owners and operators of facilities and systems in the CI/KR sectors. The scope of activities for CI/KR protection requires valid, two-way information sharing, which requires the trust that can only come with the implementation of a real partnership between the sectors and government. The Sector Partnership provides a national forum for requirements identification, planning and policy coordination, and the mutual path forward for implementation and operations for effective information sharing among the CI/KR owners and operators, federal agencies, and state, local, and tribal government.

The components of the Sector Partnership provide the policy, planning, coordination, and implementation of CI/KR protection programs and its supporting information sharing environment. These components include the following.

Sector Coordinating Councils (SCCs) serve as the government's principal point of entry into each sector to address the entire range of CI/KR protection and risk-management issues. SCCs are self-organized, self-governing entities consisting of a broad base of sector infrastructure owner-operators and their representatives from sector trade associations. Often chaired by a sector owner-operator, SCCs serve as "honest brokers," facilitating sector-wide harmonization and coordination of the sector's CI/KR protection policy development, planning, program implementation, and monitoring activities. Each SCC identifies and supports the information-sharing mechanisms, needs, and capabilities most appropriate for its sector.

Government Coordinating Councils (GCCs) serve as the governmental counterparts to the SCCs. Each GCC is chaired by the Sector-Specific Agency (SSA) for the sector, as designated by Homeland Security Presidential Directive 7 (HSPD–7) and the NIPP, and includes representatives from DHS, the SSA, and other appropriate supporting government agencies. GCCs are non-regulatory in nature, are intended to maximize interagency coordination and information sharing at the operating level, and are tasked to institutionalize a true partnership with DHS and other government partners. GCCs provide coordinated communication, issue-development services, and initiative implementation among government partners. Each GCC engages and supports its corresponding SCC's efforts to plan, implement, and execute the necessary sector-wide measures for CI/KR protection, including information sharing within the government and with the sector.

The Partnership for Critical Infrastructure Security (PCIS) serves as the cross-sector council for the CI/KR owners and operators. It coordinates cross-sector initiatives in support of public and private efforts to promote assured and reliable provision of critical infrastructure services in the face of emerging risks to economic and national security. PCIS membership consists of one or more members and their alternates from each of the SCCs.

The Federal Senior Leadership Council (FSLC) is an interagency group that consists of senior representation from each SSA. The Council addresses common issues, dependencies, and impacts that cut across the sectors. The formation of the FSLC enhances communications and coordination among federal departments and agencies with a role in implementing the NIPP and HSPD–7.

The State Local Tribal Territorial Government Coordinating Council (SLTTGCC) serves as a forum to coordinate and communicate among state, local, and tribal homeland security advisors or their equivalents, and to ensure that they

are fully integrated as active participants in national CI/KR protection planning and implementation activities. With the implementation of the SLTTGCC, state, local, and tribal homeland security leadership can engage with the national security leadership of the CI/KR owners and operators and the federal government to identify and implement an effective framework for cooperation and coordination. The result can then be tailored for regional differences that will integrate the capabilities of national CI/KR protection programs with those implemented at the regional, state, or local level.

The Government Cross-Sector Council serves to coordinate government activity across sectors. It is made up of two sub-councils: the FSLC and the SLTTGCC.

Mechanisms for Policy and Strategy Coordination

Advisory committees are a way of ensuring public and expert involvement and advice in federal decision-making. The Critical Infrastructure Partnership Advisory Council and the National Infrastructure Advisory Council allow government and owner-operators to undertake collaboration and information sharing to support policy/strategy, planning, and requirements identification.

The Critical Infrastructure Partnership Advisory Council (CIPAC) membership consists of the CI/KR owners and operator members of all SCCs and their corresponding GCC organizations. It employs a special exemption (pursuant to Section 871 of the Homeland Security Act) to the Federal Advisory Committee Act. This exemption protects SCC and GCC discussions containing sensitive CI/KR information from public disclosure, thereby facilitating regular, ongoing, and multi-directional communications and coordination.

The National Infrastructure Advisory Council (NIAC) is the President's principal advisory panel on critical infrastructure protection issues spanning all sectors. It comprises up to 30 CEO-level leaders from private industry and state and local government. The NIAC is charged with improving the cooperation and partnership between the public and private sectors in securing critical infrastructure and advising on policies and strategies that range from information sharing to roles and responsibilities between public and private sectors. In October 2005, the NIAC issued its recommendations for implementing the Sector Partnership, many of which were subsequently adopted by DHS. In addition, in July 2006, the NIAC issued recommendations regarding the Intelligence Community's coordination with CI/KR owners and operators. As a result of the collaboration between the Director of National Intelligence, the Program Manager of the Information Sharing Environment, the DHS Office of Intelligence and Analysis (OIA), and other members of the Intelligence Community, there have been significant advances toward meeting the intent of those recommendations.

Support Mechanisms

A series of operational mechanisms exists to support information sharing with the CI/KR sectors. These mechanisms consist of the organizations, processes, and personnel that support the exchange of information among DHS, other Federal agencies, State, local and tribal governments, and the CI/KR sectors. Efforts can be categorized into four broad areas

1. Content Development

Homeland Infrastructure Threat and Risk Analysis Center (HITRAC) is a partnership between OIA and the Office of Infrastructure Protection (OIP) within DHS. It provides tailored risk assessment products for CI/KR sectors, fusing consequence and vulnerability information from infrastructure protection communities collected through OIP with threat information from intelligence and law enforcement communities. It has access to a network of sector experts through the SSAs and SSCs, to specialists, and to field-deployed Protective Security Advisors to obtain CI/KR Sector expertise. Products include: (1) strategic risk assessments for each CI/KR sector; (2) threat handbooks; (3) information bulletins; and (4) analytic reports on suspicious-activity reports to sectors. Initial experience and feedback from the sectors using HITRAC products strongly indicate that it is a mechanism that delivers useful, actionable information.

Office of Infrastructure Protection Division, as a part of their CI/KR protection mission responsibility, this office develops information products on vulnerability, consequences, interdependencies, and protective strategies, as well as recommended effective practices. This information, combined with threat analysis provided through the Office of Intelligence and Analysis, results in information used by the CI/KR sectors.

The Sector Specific Agencies (SSAs) as mentioned above, are the Federal departments and/or agencies identified in HSPD–7 as responsible for CI/KR protection activities in specified CI/KR sectors. Along with other CI/KR relevant functional agencies, they bring expertise, authorities, experience, and content in participating

as partners within the CI/KR information-sharing environment. Particularly in hazards risk management beyond terrorism, many SSAs have long traditions of working with their CI/KR sector counterparts, as well as deep-seated expertise. Consequently, they have information products useful to the CI/KR sectors. The SSAs are also fully engaged as partners in the development of the Homeland Security Information Network sites, which DHS has provided each of the sectors as an information-sharing tool.

2. Information Delivery Mechanisms

The National Infrastructure Coordination Center (NICC) is the round-the-clock watch mechanism through which the National Operations Center (NOC) maintains situational and operational awareness, communications, and coordination with CI/KR partners. It provides a centralized process for coordination and delivery of information between the government and the CI/KR sectors, particularly the SCCs, GCCs, and the sector-based Information Sharing and Analysis Centers when they exist for a sector. The NICC serves as a DHS focal point for CI/KR suspicious activity and incident and status reporting; receives, logs, and tracks requests for information and assistance from the owners and operators of the CI/KR; and provides industry partners with Web-enabled access (via the Homeland Security Information Network) to DHS Situation Reports, bulletins, and other products. The NICC uses the Executive Notification System to provide rapid turn-around notifications of needed action, such as alerts and warnings.

The Homeland Security Information Network-Critical Sectors (HSIN–CS) is the primary technology tool to facilitate the information sharing necessary for coordination, planning, mitigation, and response. HSIN–CS is an Internet-based platform that enables secure, encrypted, Sensitive-But-Unclassified/For-Official-Use-Only-level communications between DHS and vetted members of the CI/KR sectors, as well as within and across the sectors. DHS fully funds and maintains HSIN–CS, thereby removing the obstacles of cost and day-to-day efforts required to support systems implementation, operations, and maintenance. DHS supports the unique requirements, outreach, and program-support needs of the CI/KR users to create robust, sector-specific information-sharing hubs for each sector. HSIN–CS includes a separate site for each CI/KR sector, designed and implemented in collaboration with the sector's GCC and SCC to best meet sector-specific needs. It also provides a top-level publishing capability to share applicable DHS and other information resources with all sectors simultaneously. HSIN–CS directly supports the building of trusted, reliable, and valued public-private sector partnerships, as well as two-way sharing of information.

Critical Infrastructure Warning Information Network (CWIN) provides a survivable network, not susceptible to service disruptions, to connect entities essential to restoring the nation's infrastructure during incidents of national significance. It connects key operational CI/KR sector entities, emergency operations centers of the 50 states, the District of Columbia, and the NOC.

3. Relationship Management

Sector-Specific Agencies (SSAs) As mentioned previously, the SSA's have the responsibility of working with each sector to implement the NIPP framework and guidance, as tailored to the sector's specific characterisitics and risk landscape. They serve as the key point of contact between the sector and the federal government to coordinate critical infrastructure protection, incident response, and infrastructure recovery.

Sector Specialists develop and sustain relationships at the national level with sector stakeholders to build trust and promote partnership. The Sector Specialist maintains extensive situational awareness of infrastructure issues and priorities. They keep a finger on the pulse of sector activities (economic, political, technological, and structural) to assess their implications on sector operations and security. The Sector Specialists are housed within the Office of Infrastructure Protection and HITRAC.

Protective Security Advisors provide field-deployed support to CI/KR owners and operators on specialized CI/KR security topics. They facilitate, coordinate, and/or perform vulnerability assessments in support of CI/KR owners and operators; they also assist with security efforts coordinated through state homeland security advisors, as requested.

4. Enabling Programs for CI/KR Information Sharing

The Protected Critical Infrastructure Information (PCII) Program provides a structure and processes to ensure that voluntarily submitted critical infrastructure information will be exempt from public disclosure, will not be used for regulatory purposes, and will be properly safeguarded. To implement and manage the

program, DHS has created the PCII Program Office within the Infrastructure Partnerships Division in OIP. The PCII Program Office receives and evaluates critical infrastructure information to determine whether it qualifies for protection under PCII. The Office also manages a certification program for other Federal agencies and States to receive and manage PCII-protected information.

CI/KR Classified Security Clearance Program provides a capability whereby the federal government can discuss and share classified information—on vulnerability and consequences, as well as threats—with the owners and operators of the CI/KR. The owners and operators of the CI/KR will always have the primary responsibility for managing the risks of their own assets, systems, and functions. They also have current information on their operational and business processes, the usage and application of technology in their CI/KR sector, and what is most critical to their operations, including dependencies on other sectors and locality to locality variations. The Classified Security Clearance program is sponsored, coordinated, and funded by OIP. It is implemented through DHS's Office of Security and its policy and procedures framework.

CI/KR-Unique Policy and Legal Framework

For CI/KR owners and operators, sharing information with government at all levels creates a range of risks affecting the viability and efficiency of their business operations, including liability risk, antitrust risk, and competitive risk.

The risks associated with liability and competitiveness are the primary reasons that infrastructure owners and operators seek ownership and control over CI/KR data that they submit to government. They want to know who gets the information, what is done with it, and how is it protected from inappropriate disclosure. These assurances, to the extent possible, are necessary for building trust in government institutions and processes that receive and handle voluntarily submitted CI/KR information.

The Information-Sharing Environment

Our information-sharing efforts are part of the broader Information-Sharing Environment (ISE) created by the President in accordance with the Intelligence Reform and Terrorism Prevention Act of 2004. The purpose of the ISE is to measurably improve information sharing between and among the Federal government, appropriate State, local, and tribal officials, and private-sector entities. In recognition of the important work under way in this area under the NIPP framework, the program manager for ISE, in coordination with the Information Sharing Council, has officially designated the CI/KR NIPP process (as described above) as the mechanism in which the private sector will be incorporated into the ISE. In this role, the NIPP Partnership Framework provides guidance for the private sector to engage in ISE-related policy, governance, planning, and operational coordination, as well as a forum for identifying and satisfying information requirements.

Particularly critical is the coordination of CI/KR information sharing at the national level with that at the local level, where most decisions are made and actions taken to support CI/KR protection. The implementation of the ISE and the formation of the State, Local, and Tribal Government Coordinating Council as a key component of the Sector Partnership are critical to this necessary coordination. Consequently, the integration of the CI/KR information sharing framework into the ISE as its private-sector component strengthens the foundation for effective coordination.

In addition, OIP works closely with and supports Assistant Secretary Charles Allen and OIA in DHS's efforts to use and integrate into State and Local Fusion Centers. The OIP exchanges information with the Fusion Centers using existing channels such as the NICC and HITRAC.

Sustainable Information Sharing

The foundation for sustainability of CI/KR information sharing comes from leveraging the structures, processes, and mechanisms for responding to natural disasters and accidents. When there is a terrorist incident, the tools will already be in place, the training will be complete, and the familiarity and experience required to efficiently implement defined procedures will already be established.

The NICC has undertaken a comprehensive effort to identify relevant and useful all-hazards information available from agencies within DHS to populate CI/KR portals on HSIN–CS. The NICC is the DHS CI/KR hub to ensure that DHS-sourced information remains current. Additionally, OIP has undertaken a project to generate various operational products for CI/KR derived from resources freely available in the public domain. These will include specific products requiring open source research and analysis, as well as a currently available daily reports.

The sectors themselves determine appropriate and useful content for their sector. Some of the SSAs produce sector-specific, non-terrorism related informational prod-

ucts that other sectors find useful for situational awareness and management of incidents related to their CI/KR. Both public and private partners within the sector work with DHS to identify the functional and security capabilities to enable the storage and management of their information on HSIN–CS, as appropriate.

Measurement of Effective Information Sharing

The goals for information sharing in the CI/KR environment are effective and efficient protection, preparedness, response, and mitigation of consequences to incidents that could disrupt the nation's CI/KR. The Sector Partnership represents the foundation for these activities and the information sharing that supports them. Change is a constant: the threat evolves; industries evolve, and the environment within which businesses must operate and provide services and products to the nation evolves. Information requirements will change accordingly. Successful information sharing is measured by the outcomes associated with protection, the efficiency and effectiveness of actions taken, and the adaptability of the entire structure of the Sector Partnership and its supporting information-sharing mechanisms.

With a clear focus on the desired outcomes of protection, and a foundation for systematic engagement and relationships based on trust, an information-sharing environment for CI/KR can sustain itself, adapt, and protect the nation's CI/KR and its citizens.

In closing, I would like to assure you that DHS is relentless in its work to continue building a strong, positive partnership with the private sector in which valuable, actionable information can be shared with the right people at the right time to ensure the protection of our nation's most valuable CI/KR. Our country deserves nothing less. I thank you for your time and appreciate the opportunity to answer any questions you may have.

Ms. HARMAN. Thank you all. I will now yield 5 minutes to myself for an opening round of questions, and all will participate on the same basis.

Mr. Chaparro, I appreciated your opening comment that the mission of your department is 24/7 to protect the security of Americans. I think that is the mission of the members here, too, and I would hope that you see this hearing exercise as a collaboration. We want you to do your jobs better, and I hope you want us to do our jobs better because this is a hard task.

I did read the 50-page NIE last week, I thought it was a very good work product, but as we all know it doesn't have names, addresses and serial numbers. The threat is greater, but we don't know where attacks could come. I am one who is quite pessimistic about our ability to keep our entire country safe from those attacks if those who want to attack us are prepared to take their own lives, which they are. So we all have to collaborate better, and we certainly have to get information to the private sector that is as good as we can field.

In that connection, let me make two comments. First, a thank you to your Secretary, Michael Chertoff for, spending last Friday at the Port of Los Angeles and in some other meetings in Los Angeles. We were talking about the need to resume trade promptly should the port complex of LA in Long Beach be attacked, either a terrorist attack or some natural disaster. And I think that all of us are learning together that what needs to be done in the private sector plays a major role. So a public thank-you to Michael Chertoff for spending the time in my area.

Loretta Sanchez, a member of this committee, who chairs our Port Subcommittee was also present, as was another member, Dana Rohrabacher, who represents the physical port infrastructure. At any rate, thank you for that.

Second comment, as a member of the Intelligence Committee for 8 years in the House, I have read a lot of intelligence products, and

I always used to say that some of the best information I got was not from them, but was from watching television, these major news channels, CNN and others.

In that connection, you will hear—I assume you are sticking around for the second panel—some testimony from Lester Johnson, who is the Manager of Investigations and Crisis Management at the SCANA Corporation, a $9 billion Fortune 500 energy-based holding company. Let me quote from his prepared remarks:

"I am forced to rely on the open sources of information to receive most of the situational awareness information available. I have found a television tuned to a cable news network provides the most efficient, timely and accurate information to my company. Considering the amount of investment our country has made toward the sharing of information among government agencies and the public sector, I find this reprehensible. We are certainly capable of embracing technology and conducting ourselves better than that."

Now, I take this as a constructive comment, and I would like to ask the entire panel to comment on it.

Mr. CHAPARRO. I think that he's absolutely right, there are a lot of things that we need to do better.

We do rely on open source information to help inform our analysis. The threats that we see, as you pointed out, are often nonspecific, and we must continually balance the need between putting out information that will help people take relevant steps to mitigate threats versus creating a panic atmosphere that will cause people to expend resources unnecessarily.

Oftentimes, the reports that we see in the news media, as you are well aware, are very, very good and sometimes the facts aren't quite all there, and we have to—before the government steps in and releases information, we need to try and make sure that information is as accurate as possible, while trying to maintain the timeliness and relevance.

Ms. HARMAN. Thank you.

Mr. CHAPARRO. Clearly, we have work to do. Our dissemination mechanism is not as efficient as putting something out over the airwaves. We sometimes wish they were, and do face challenges in that area.

Ms. HARMAN. Do the other witnesses have comments, as well, briefly?

Ms. SMISLOVA. Yes, ma'am. We do attempt to contribute to the body of information that's available to the private sector, to the news media, by providing something that we think is more authoritative and more value added.

A point that I forgot to mention in my opening statement is that over the last 2 years HITRAC has done many of our products, over 40, with the FBI. Many of those deal with the events that the media is covering. We try to get more information that is not readily available to the private sector from the media.

Ms. HARMAN. Thank you.

Mr. Caverly.

Mr. CAVERLY. I don't think we will ever have the agility of a cable news network for the very simple reason, they are on the scene, we still have to get the reporting in. As I pointed out, there are different levels of information, so there is that tactical imme-

diate information which we and them are learning from what is happening.

I would argue, the strategic information is something different; that is where the analysis fits in. If you think back to the early 1990s you were worried about an abandoned car sitting in front of your factory. Then you were worried about the car that came that came screeching up and somebody ran away. You are now worried about somebody driving through your gate. Those are all evolutions on the strategic level, and I think our analysis is the supporting information that gets out to the strategic level, so there is a mix in what you are discussing.

Ms. HARMAN. Thank you very much. My time has expired, I now yield 5 minutes to Mr. Reichert.

Mr. REICHERT. Thank you, Madame Chair.

And thank you again for being here this morning.

I understand the complicated process of gathering intelligence and looking at leads and figuring out which leads are important, which leads should be shared with members of our community.

In a case that I worked back in the 1980s, it took us 19 years to solve, with 40,000 suspects and 10,000 items of evidence; it was a complicated case. And sorting out information is tough; and who to share it with is the other thing and trying to keep it from the people trying to get it is a whole other matter.

I noticed a couple of times our witnesses, our panel this morning, mentioned the information must be relevant, actionable, it must be timely; and another way it was phrased was situational information, situational assessment, strategic information and tactical, actionable information. But then I hear that these things are critical.

But did I misunderstand you when you mentioned—I am sorry, I am not going to pronounce your name correctly, ma'am—that all information flows through Charlie Allen?

Ms. SMISLOVA. All intelligence information, if it is intelligence. Then we are under the same rules as the rest of the Intelligence Community.

Mr. REICHERT. Does that include every classification of intelligence that goes through Mr. Allen?

Ms. SMISLOVA. Most of what we produced is at the FOUO level, over 80 percent of our production. Much of that, however, is based on classified intelligence information. It has been downgraded.

And that is another key role we believe we are serving for the private sector. I have access to all available information about this particular terrorist enemy, but I am able to broker some of the information to be downgraded to an unclassified level, the actual data about specifics, about attack methods, et cetera, not sources and methods.

Mr. REICHERT. I just wonder if—that is, when we talk about timely information, if we have one person who it is flowing through, whether that is a little bit of a choke-point.

Ms. SMISLOVA. It has improved considerably. We did very well with the London timelines.

Mr. REICHERT. Yes, you did. I have had experience with that in my previous career.

There is also mention of a National Coordination Center where information flows out. How does that operation work?

Mr. CAVERLY. The NICC is a watch and warning center. They are a hub. We use them as our operational entity to move information out to the private sector, whether it is going to sector—lists of participants in the sector given by the sector coordinating council, participants in an information and sharing analysis center and other people. We have built lists' connectivity and expanding that, working with each of the councils, to make sure we can get down to the operational level.

We think with the institution of fusion centers, which operate at that local level, we will expand that reach significantly.

Mr. REICHERT. So as we begin to share and learn what information we can share, an important thing, as Mr. Chaparro mentioned, was the mitigation strategy and the input of the private sector.

What is your plan to improve that process? And of course, Mr. Caverly, you mentioned it was built on trust. I think, all three of you, there is a need for this mitigation strategy; that is, the key part of this whole thing in sharing the information is to mitigate the events.

What are your future thoughts on how that program would come together?

Mr. CHAPARRO. Well, the keys have to be multiple. The private sector is very diverse and has multiple needs, everything from technical, what is happening now, to what do we need to do 5, 10 years from now. The relationships must be built on trust, and there are a number of governance mechanisms through the ISACs, for example, where we are in constant exchange with the private sectors.

But also we are really aggressively reaching out through the State and Local Fusion Center Programs because we can do that at the local level, which is where the action really takes place and where people need to really know that information. By putting people forward in fusion centers, we will have the ability to establish those trusted relationships that Mr. Caverly mentioned as being so important.

Mr. CAVERLY. Let me also point out, prior to 9/11 and the creation of the Department, that the structure that was being used was one in which we take an intelligence product and fundamentally throw it over the transom to a group of experts in the sector for them to work a second time.

With standing up HITRAC, with being able to give security clearances, we didn't feel we needed a two-step method. We bring in those experts from the sector, so we are working together to figure out, is it both relevant to their concerns and is it communicated in a way that makes sense to them. Because as I said, talking to a nuclear power plant operator, I am using a very different vernacular than someone in a water system.

So we bring them into HITRAC. As we get more experts, we will expand that base, but that is the point of structure of what we have put in HITRAC is to be able to do that and do it collaboratively.

Mr. REICHERT. Thank you.

Madame Chair, I have seen a great deal of improvement, and I am happy to hear you use the fusion center as your conduit.

I yield.

Ms. HARMAN. The gentleman's time has expired. I now yield 5 minutes to Mr. Dicks for questioning.

Mr. DICKS. The National Coordination Center, Information Sharing and Analysis Center, Sector Coordinating Council, specific sector agencies, the Department's private sector office, HITRAC, HISN, FEMA's emergency support function, ESF and others. In a word, it is not one-stop shopping.

Would you agree with that or do you think this has gotten—I mean, aren't there a lot of different places people go?

Mr. CAVERLY. I don't think it is so much a question of different places where people go—again, they go to the people they know.

What it really is, is there are different roles played by participants in the process and different equities. If I am responding to a natural disaster, FEMA is bringing expertise that is different from the Intelligence Community if it is not a terrorist event.

The Sector Coordinating Councils for executive bodies, they give us senior guidance that allows us to look to see what is appropriate for the water sector or the nuclear sector. The ISACs provide a framework in which we can communicate with and provide the channel for that communication.

So while it looks confusing, we believe that as we continue to work through the model we have put together, each of those people has a role to play.

I recognize there are some processes over time, but again, my responding to a strategic terrorist threat is probably very different than I will be responding to a catastrophic event or something else; and we need those different expertises and mechanisms in a coordinated fashion and that is what we're working very hard to do.

Mr. DICKS. How does a private sector company know which outlet is the right one to go to not only to obtain information about a threat, but also to feed relevant information to the Department?

Mr. CAVERLY. That is exactly why we established the NICC as the one 7/24/364 center that they can plug into. It is our job to direct them to the right people. So between the NICC and my sector specialists who support them, we facilitate that conversation and get them to the right place. It should be our job to understand the internal workings of the Department, and we should support the private sector when it gets a problem.

Mr. DICKS. Ms. Smislova, is the focus of HITRAC intelligence products more on the operational side, meaning, do they tell folks in the private sector what to do or are they aimed more at providing situational awareness?

Ms. SMISLOVA. They are focused primarily on providing the private sector with information about the adversaries so that is information that can lead them to decisions about what to do. We do occasionally offer our assessment of what mitigating factors would work, but I would say it is difficult to characterize all of our products one way or another.

We have several different kinds of products, but mostly we are in the business of providing the private sector with intelligence-derived information about the international terrorists and their affiliates, information that the private sector does not have ready access to.

VerDate Nov 24 2008 10:54 Aug 17, 2009 Jkt 000000 PO 00000 Frm 00028 Fmt 6633 Sfmt 6601 H:\DOCS\110-HRGS\110-62\48957.TXT HSEC PsN: DIANE

Mr. DICKS. Ms. Harman, the Chair, got into this, but I want to go through it again. There is concern in the private sector that HITRAC is not providing reports in a timely fashion. What are you doing to work on that? I mean, do you talk to the private sector about this?

Ms. SMISLOVA. We do. We do. And then after an event such as the attempted bombing in London and Glasgow, we have canvassed our private sector customers to ask them to reevaluate what we did and how we did it. At that particular event, we changed some of our own processes. In working immediately with the FBI—we have developed a very close relationship with our sister office at the FBI that also analyzes threats to infrastructure, so we had developed some better processes.

We are aware of a request for more timely information. Again, we do view our role as being more authoritative, when we do say something we try to have more information than is available in the media. Although if we don't, then we will just report that.

In addition to——

Mr. DICKS. You said Charlie Allen is doing better. Did you give him a speed reading course or what did you do?

Ms. SMISLOVA. No. No. Some of that is delegated.

I want to make sure that people understand HITRAC isn't its own little office without allegiance to the regular intelligence requirements that all of us in the Intelligence Community are supposed to adhere to, so all of our products are properly vetted and properly sourced and then go out in a proper fashion with the correct classification.

Mr. DICKS. I am glad to hear that you are cooperating and working with the private sector. I find that DHS has some difficulty in other areas doing that effectively; and it bothers me that there is kind of—I sense a rigidness in the agency in terms of being responsive and taking into account what the private sector is saying and a lot of our fields talk about fingerprinting and the border security issues, things of that nature.

But I think it is very important that you work with your customer. I think anybody who does a good job listens to their customer.

Ms. SMISLOVA. Yes.

Mr. DICKS. Thank you.

Mr. CAVERLY. Madame Chairwoman, I just want to underscore one thing we have and take very seriously in the Department: the duty to warn and the responsibility we are given with legislation.

There are a large number of incidents in which we have specific information that affect a specific entity. In that case, I believe that the speed at which we get to those people is very good. It is not in the public domain; they are very focused when you have the name of a specific target or specific organization.

We go out, we use the ability, Mr.µAllen is on the phone with them very quickly, we can use our PSAs. That is a piece that doesn't see the light of day and we are happy that it doesn't.

Mr. DICKS. That is good to hear.

Ms. HARMAN. I thank you for that additional comment. A lot of the successes of the Intelligence Community are not known and that is how it should be. It is a little tough when one's perception—

the perception of many is that there are only failures, those of us know there are also successes. I think you have pointed out some areas of real progress.

I appreciate your testimony, Mr. Caverly, about the security clearances. One of the things we want to work on here is to change our classification system so that it is simpler and so that it is not used as a turf protection system. Things should only be classified to protect sources and methods; I know you all understand that. We do support protecting sources and methods, but we are preparing legislation here, and will hopefully introduce it soon, based on a careful hearing record that will make that system easier to navigate. Meanwhile, it is very important that the private sector have access, as appropriate, to classified material.

I now yield 5 minutes to Mr. Carney for questions, and will point out to this panel and to the second panel that I have to leave in 5 minutes to go to a markup at another committee, and Mr. Carney will assume the Chair.

Mr. Carney, 5 minutes.

Mr. CARNEY. Thank you, Madame Chair.

Mr. Caverly refers to the one-stop shop. Is that NICC, is that how you describe it?

Mr. CAVERLY. What I would say, the one-stop shop that is the central place you go into. The products—if we are sending something out, I send it through there, but if I have to connect somebody who has a question about a specific thing to that, so it is a central point, that then reaches into the Department.

Mr. CARNEY. So as a private sector individual or business leader, I would go to the NICC for information?

Mr. CAVERLY. For issues relative to infrastructure protection and those issues, yes.

Mr. CARNEY. So in a sense, to use sort of the techie vernacular, you are kind of a router, NICC is a router of information?

Mr. CAVERLY. As I said, I don't believe we should expect the private sector to understand the arcaney of the Department.

Mr. CARNEY. Thank God, we all struggle with that. I worked for DOD myself so I could navigate that.

One other question I had: How much duplication of effort is there? There seems to be a lot of potential—this is for everybody, by the way—crossover here. How do we sort that out? Is there a snarl that we can do better with?

Mr. CAVERLY. There is no doubt there are areas of duplicated effort in what we are talking about today, because the leadership had the foresight to set up HITRAC where we put together both the intelligence function and the capability of getting—if you want the expertise of this sector, I think we have eliminated the duplication, because they work well together and they have the ability out of HITRAC to reach back into the deeper parts of the organizations that support them to get deeper.

So the whole point of HITRAC was to ensure that we had the coordination, got it to be efficient and eliminate that if you want competitive duplication.

Mr. CARNEY. Is it working?

Mr. CAVERLY. I believe it is working and the products we turn out to the private sector are a good indication of that.

Mr. CARNEY. Ms. Smislova.

Ms. SMISLOVA. I also agree that it is working, and for the most part, there is no duplication. We are one of the few Intelligence Community entities that writes for the private sector, and that does mean that our products look different than many of our other Intelligence Community colleagues.

Our customer is much more interested in what the enemy is learning—tactics and techniques and procedures—and they are not as interested in the sources or methods. Again, that does help us facilitate the production of FOUO material, but they are very specific in their interests and I think that is very useful for us in avoiding its duplication.

As Mr. Caverly mentioned, I am in charge of the IA part, as well as the IP portion of HITRAC, and I ensure that we are not doing the same work. We are not large enough to do that. Thank you.

Mr. CHAPARRO. I don't think Ms. Smislova has the resources to duplicate efforts.

If there is a challenge that we face with HITRAC, as I said earlier, the private sector is so diverse, and the types of information that are needed, for example, in the nuclear sector versus what is needed in the agricultural sector or the finance sector really pull in different directions. But the fortunate thing about HITRAC is that you are marrying up Intelligence Community officers, professionals, along with sector specialists who understand the vulnerabilities, who understand how the systems work, how they interrelate and how they operate. You are marrying together the understanding of the threat and what the adversary is trying to do, along with the expertise from the critical infrastructure sectors, and generating products specifically for the private sector; and that is unique, and I think that is what is working.

Ms. SMISLOVA. I wanted to add, if I may, that I also believe it makes us much more efficient than many of my other colleagues, because we do have that synergy and it has proven to be very effective.

Mr. CARNEY. How much of a dialogue is there with the private sector? I know you push out information, but how receptive are you to information from them?

Ms. SMISLOVA. We are interacting with different members of the private sector daily. Some of the private sector entities have organized conference calls which we conduct weekly, for example, with the chemical sector. The nuclear industry arrives monthly for a classified briefing; we brief the Sector Coordinating Councils; whenever we are asked, we send people to different private sector conferences to specific companies, so I would say daily. In addition, we are talking to the States about their critical infrastructure.

Mr. CAVERLY. I was in a meeting of the water sector coordinating council. We were giving them the classified brief earlier this week, and what was pleasant about the brief was a discussion about a specific issue in which the analyst talked about how she had reached back down to the local level, talking both to utility and to law enforcement to pull together and get the information appropriately.

Can we do more of it? Of course we can as we get better and get the networks built. I think the foundation is very solid and the

structure that we have put in place is the structure that lets us now amplify that and get to a much broader base.

Mr. CARNEY. That is absolutely important, that we have the avenues by which local and State officials certainly and the private sector can give you assay as well. Your job is to provide them assay, and they do the same.

Mr. CAVERLY. Well, I think one of the most important things is the ability to turn a product out that, in essence, informs the private sector, and they understand the information they have goes in and they get something back for what they give us, they get the analysis.

That has not been, historically, something government has done well. We are working hard to do that, because they devote the time to give us something, we owe them. Hey, it means something or it doesn't mean something; that is a new track for us. They do it very well, but it is also a self-fulfilling prophecy, the more that they give us, the more we give them back answers; the more we give them back answers the more they give us. And we are building that.

Ms. HARMAN. I think we will leave the first panel on that note.

Mr. DICKS. Are you sure? You said there was a dialogue there that you didn't have enough people to do both.

Ms. SMISLOVA. No. We are growing, we continue to grow.

Mr. DICKS. Do you have a lot of positions unfilled?

Ms. SMISLOVA. No, I do not, but we are continuing to grow and our mission continues to expand. All the critical infrastructure of the United States is in a State, so in addition to talking to the private sector, if we go to a State, then we do talk to the State officials as well.

Ms. HARMAN. Thank you. And thank you for inviting an ongoing dialogue. I hope you can stick around for the testimony of the private sector and maybe a conversation with some of the private sector witnesses, because the goal here is for all of us to do a better job, 24/7, of keeping America safe.

This panel is excused, and Mr. Carney will take over the Chair for the second panel. Thank you.

Mr. CARNEY. [Presiding.] We will begin the second panel now. I would like to welcome, first of all, Mr. Lester Johnson, who serves as the Manager of Investigations and Crisis Management at the SCANA Corporation.

Mr. Johnson leads a staff of professional investigators who conduct investigations, internal corporate compliance issues, criminal violations against the corporation's property or personnel, executive protection, background investigations and risk reduction efforts on behalf of the corporation. Mr. Johnson is responsible for the development and continual assessment of security risk management and reduction plans for the critical infrastructure operated by his company.

Our second witness is Mr. John Meenan. He serves as Executive Vice President and COO at the Air Transport Association of America, ATA. He is responsible for ATA operations, with a particular focus on technical safety, security, environmental, economic and legal policy issues impacting the airline industry. Mr. Meenan joined the association as Assistant General Counsel in 1985 following 9 years with the U.S. Secret Service.

Our third witness, Mr. Rich Hovel, is a Senior Aviation Homeland Security Advisor to the Boeing Company. Prior to his tenure with Boeing, Mr. Hovel served as the Federal Security Manager for the FAA, Aviation Security Operations Division at the Seattle Takoma International Airport. Mr. Hovel began his law enforcement career with the Albuquerque Police Department; afterwards he worked for the Idaho State Police as a trooper and supervisor and criminal investigator.

Without objection, the witnesses' full statements will be inserted in the record.

Mr. CARNEY. I now ask each witness to summarize his statement for 5 minutes, beginning with Mr. Johnson.

STATEMENT OF LESTER J. JOHNSON, JR., MANAGER OF INVESTIGATIONS AND CRISIS MANAGEMENT, SCANA CORPORATION

Mr. JOHNSON. Thank you, sir. Chairman, it is truly an honor and privilege to appear before you, and I appreciate the invitation to do so.

We have for some time been challenged, I think for all of us, the people here with me now, the panel prior to me, this is a very challenging issue which all of us face.

Mr. JOHNSON. And it is a very difficult issue, and I want to recognize that the members of the panel before me I think spoke very eloquently and the fact that they are making progress and that we are very appreciative of their work. We understand the difficulties they face. We too face difficulties. We are charged with the protection and the security surrounding some of the most critical infrastructure that this country has, and we too take that very serious as well. I know that they are very inept and attuned to what our needs and they are working diligently with each of these sectors. And as many of them said today that there are very many of those and they all have very differing needs and requirements. But we still have work to do, no question.

I think in the area that was brought up by one of the committee members earlier, I call it almost portal fatigue. We are in a position now that with information being pushed back into homeland security as being sent out in a sundry of ways in a lot of different portals and it takes a tremendous amount of effort and time on our staff's part to go out and I call it chase or find this information, versus having made potentially a role-based security where that information could come into a dashboard that we could go to one place and feed the information that we require or any of our other sectors may require and go to one place and have that pushed down to us I think is something that we all need to focus on and work toward. We have done this successfully in other areas within our corporation and I know some governments have done this as well, so I know the technology exists to do that, and we just need to put our heads together and work toward that effort.

The flow of information and the timeliness is probably the area that I have the most heartache with. It is very common that when I find information out, it is through open source information such as Cable News Network and other entities, and then it is very difficult to go back in and to find information or a contact person at

that point to assure that that information being reported is accurate and timely. We are not so much as concerned about the analysis of that information as we are being aware of an event and being able to take mediation steps to secure any of our like infrastructure that may be under attack or may be a subject of interest in other areas, both domestically and internationally. I don't want to wait until we have an issue to respond to it. And my goal is that we proactively go out and make that target hardened to the point that no one is going to come after it. And it is very important from our standpoint that we know about those events quickly and accurately so that we can respond in that way and secure that information.

The information sharing of the private sector, we are very fortunate in our State. Our State homeland security adviser is very attuned to this. Having the experience of working for the State law enforcement division for 28 years in my State, I have had the opportunity to serve on both sides of this issue, to both provide these services to State and local law enforcement and private sector and now from the private sector side as being involved in forwarding that information back. We have an excellent relationship on the State level. I will tell you that I think we are one of any other possibly that has a presence in our State fusion center representing our corporate and our private sector within the State. This is tremendously beneficial, and one that I would encourage Homeland Security to take that as a role model and to push that out to other States because we receive a great deal of benefit from that. We have eyes and ears in that fusion center that are getting realtime information, but we are still not getting that timely report back out from Homeland on some of the analytical information that we are looking for when that comes back.

[The statement of Mr. Johnson follows:]

PREPARED STATEMENT OF LESTER J. JOHNSON, JR.

Madam Chairwoman Harman, Ranking Member Reichert, and distinguished members of the subcommittee, I appreciate the invitation to appear before you today, as it is both an honor and a privilege to be here today. I would respectfully request that my written testimony be submitted into the record. I appear before you today to share some insights I believe are critical to the private sector information sharing and to highlight those areas in need of improvement and those which are on the path to success. The private sector currently has sole possession of approximately eighty-five percent of the vital critical infrastructure in existence today, upon which all of us depend on daily. For a number of years now, we have been focusing on how to build trusted relationships and processes to facilitate information sharing; overcome barriers to information sharing, clarifying roles and responsibilities of the various government and private sector entities that are involved in and charged with protecting critical infrastructures. In order to protect our nation's critical infrastructure and key assets (CI/KA), the full support, cooperation and engagement of Government and the private sector partners at all levels is required.

I have the unique opportunity to speak to this issue from both the government and private sector due to my previous employment history with the South Carolina Law Enforcement Division (SLED) and my current employer in the private sector. I had the opportunity to participate in the delivery of services with respect to Homeland Security in South Carolina as SLED is the designated agency responsible for Homeland Security and Chief Robert M. Stewart serves as the State Homeland Security Advisor. The importance of trusted relationships between Government and private sector in South Carolina has been recognized and established on several levels. Private sector representation exists on both the regional and state Counter Terrorism Councils and in the all source Fusion Center. I will elaborate more on these

initiatives later in my testimony. Below, I will be identifying areas of both concern and success, as it is my intent to be a part of the solution to these areas.

Information Flow:

The flow of information between the Government and private sector are interpreted to be a one way investment for the private sector. While there is a great effort on the Government's part to solicit situational awareness, timely and actionable and proprietary information from the privates sector, there still exists a significant deficiency on the Government's part to share the information back to the private sector. Information provided by the private sector with regard to suspicious activity is received by the Government and subjected to an analytical process which I am told includes a human and technological assessment, often taking weeks or months to complete. During this time, the information is not shared among the peers of the sector due to the lack of a complete analysis being available. Disparately, should the same information be collected by a peer member who does not forward it to the Government, there is no link identified since the Government chooses to hold the information instead of sharing it across the sector. The process I described creates an atmosphere of difficulty for the private sector to adequately place a remediation plan into effect.

I made a valiant effort to seek input from my peers in the industry who are not present here today before the committee. I have been educated on several instances where information was discovered; often months after the Government learned it, where no one the industry was made aware of an existing threat or vulnerability that could have an enormous negative impact on the industry.

Portal Fatigue:

The industry as a whole has been besieged by the number of information sharing portals from the various Government agencies and some private as well, in attempt to go and find the information. Each portal has a separate vetting process which must be adhered to, a separate user name and password, a unique URL, and to some degree each contains the same information with regard to its informational value to the user. As I am sure you aware, in the private sector, time is equated to money. There is no effort among the Government to coordinate the efforts among the various agencies to simplify this process in any way. Actually, there appears to be competition to see which agency can turn out the most portals in a given amount of time. The idea of posting the information, particularly information with no or little classification, to site for all to come to is at best a backwards approach to information sharing. One would consider the Government as the provider of information in this scenario, yet the provider creates technology requiring the end user to come to the Government instead of the Government pushing the information to the end user. A definite confusing demonstration of a product chain and certainly one the private sector is weary of. Perhaps consideration may be given to using the existing technology to develop a "role based security dashboard" atmosphere. A role based security dashboard would have an individual vetted for all the existing Government portals. The Government would then feed the information into a dashboard which would be accessed by the end user. All the information pushed to the dashboard would be available at one location, requiring one user name and password, and would provide a timely and accurate assessment of all information and could also provide tools for data mining the information based on the user instead of the provider.

Private Sector Information Sharing:

The private sector has found success in utilizing services from other private sector organizations that provide situational awareness and information on a variety of topics and services. These services, while costly to an organization, are very timely and efficient. The services allow the sector to choose the type of information they wish to receive and allow information to be vetted by the distance from a facility or city. I have personal experience with one such organization and found the services to be very beneficial. These organizations leverage technology in various formats to push this desired information out to the end user and have demonstrated an uncanny ability to learn of potential threats, delays and risks in record time.

I am forced to rely on the open sources of information to receive most of the situational awareness information available. I have found a television tuned to a cable news network provides the most efficient, timely and accurate information to my company. Considering the amount of investment our country has made toward the sharing of information among our Government agencies and the public sector, I find this reprehensible. We certainly are capable of embracing technology and conducting ourselves better than this. At a minimum, perhaps the Government should consider contracting the services of one of companies who have perfected this and make the

services available to the end users who require it. The Southeastern Emergency Response Network is another example of a creation of a private sector initiative which became necessary due to the failure of a Government effort. Homeland Security Information Network—XXX was an original effort to provide a means of information sharing between the Government and private sector. I was approached on the State's behalf to develop the program in South Carolina. I received the organizational chart for the critical infrastructure and contacted our local private sector and sought the commitment to serve in the leadership capacity for the required vetting among the sectors. Once in place, I delivered the chart as requested only to find there had been technological setbacks that would delay the initiation of the project. Some years later I was finally notified that the program would be replaced with anew program which to date has yet to be introduced.

Many of my peers and I have begun a very basic method of information sharing among ourselves as a result of not receiving the intelligence we desire from our Government sources. We have resorted to a telephone tree of sorts to ensure each of us share the information in a timely fashion and develop actionable plans for remediation where appropriate.

Dam Sector Working Group:

Several members of our industry were recruited to participate in a working group to develop the Homeland Security Information Network—Dam Sector (HSIN–DS) and the Asset Identification Database. These efforts were met with great enthusiasm by the sector and several individuals provided a great amount of resources toward this effort. Unfortunately, the Government has not provided the same level of enthusiasm and effort. As a result the project has been at a stand still for some period of time. Initially, there were technology setbacks which over time were able to be corrected. The vetting process presented difficulties over which process would be used by both entities. Due to difficulties arising from the PCII, private sector representatives are skeptical about placing the information into the system. As you can see, there are a number of issues outstanding concerning this project, which is paramount to the safety of one of our most critical infrastructures.

HITRAC:

The creation of a partnership between the Department of Homeland Security's Office of Infrastructure Protection and the Officer of Intelligence and Analysis to provide a tailored risk assessment product for CI/KR sectors fusing consequence and vulnerability information with threat information is an excellent plan of action. We continue to fall short on the timely sharing of the information generated from this program. We have been told to expect informational bulletins, analytical reports and annual reports and to date we have not received any. The sectors can only respond to strengthen and protect our infrastructure if we receive the information derived from the process below. Without the benefit of this, we have relied heavily on our own resources and our peers for information. Additionally, the lack of communication creates a large void of information flow from the private sector to the Government.

Infrastructure Information and Collection Program:

The Protected Critical Infrastructure Information (PCII) has failed to demonstrate the Government has the ability to provide a safe and secure atmosphere for descriptive and proprietary information to exist in a repository. Efforts to identify and prioritize national and sector level CI/KR information have yet to demonstrate to the private sector that the information can be maintained in a confidential manner. Recently, this was demonstrated to a peer of mine while attending a meeting, at which time a document that had been provided under the protection of this program was produced by an individual who should not have had access to the document. Incidents such as this are many and cause the private sector to withhold information which in any way may be considered private or proprietary.

South Carolina All Source Fusion Center:

Among the difficulties we face every day, there are efforts which demonstrate the success and progress we have reached at the State and local level. The creation of the Fusion center in South Carolina is a foundation for the development of a trusted relationship between Government and the private sector. I received notification only three days ago that the Department of Homeland Security State and Local intelligence Community of Interest has cleared the way for private sector representatives to be co-located within the State Fusion Center. A program such as this will greatly enhance the flow of information between Government and the private sector.

South Carolina Information Exchange:

Homeland Security in South Carolina developed the South Carolina Information Exchange (SCIEx) within the State operated all source Fusion Center. SCIEx is an excellent example of information sharing in a near real time environment. Law Enforcement agencies within the state have participated in this project by allowing the information contained in incident reports created in an automated environment to be replicated to a data warehouse with SLED and allowing for the querying of the information contained therein through a secure web browser. The sharing of this information is a tremendous resource for both the state and the private sector. Information derived from these reports can easily be placed into geographical information software and immediately demonstrate a potential threat and vulnerability to our facilities throughout the state. The technology for accomplishing this feat was developed with the assistance of the National Law Enforcement and Corrections Technology Center—Southeast, which is funded in part by the National Institute of Justice. The software code for this is an open source product, making it available to entities free of charge, resulting in the State of Tennessee initiating a project to replicate the success there as well. I have no reservation recommending this technology be used to better facilitate information sharing among the private sector. There is a success there waiting to happen without the demand of additional tax dollars and development time.

Conclusion:

In conclusion, I feel that it is imperative for the committee to understand the commitment and dedication of the private sector has with regard to the sharing of information. We realize there are great benefits to be reaped by both the sector and the Government in the presence of a trusted partnership. There have been many, too many actually, attempts to develop and implement a program where this type of exchange can be conducted and the information shared can be relayed and maintain the integrity necessary for the public sector. I and many of my peers are fully prepared to again tackle these difficult issues so long as there is the same level of commitment from our Government counterparts. Until such time, we will continue to make progress with our State Government partners and our industry peers to ensure we have the necessary information to complete our duty to protect the critical infrastructure of the United States of America.

Mr. CARNEY. Thank you. I now recognize Mr. Meenan to summarize for 5 minutes.

STATEMENT OF JOHN M. MEENAN, EXECUTIVE VICE PRESIDENT AND COO, AIR TRANSPORT ASSOCIATION OF AMERICA

Mr. MEENAN. Mr. Chair, members thank you very much. I am pleased to be able to report that from the perspective of the airline industry, the information sharing system in place today is working very effectively, in part because of the business that we are in and the focal area of activity that has been post-9/11 has had the benefit of working very closely with both TSA and DHS literally from their startup, and as a result, the system that we have developed is working I think quite effectively.

I would mention, for example, that the day of the Glasgow bombing, before I heard the report on the radio, we were already called to a conference call with TSA to discuss the implications of that for the industry. The flow of information is very good. The exchange of information is very good. We, in fact, report security incidents on a regular basis to the government. They are processed. They are looked at for a variety of different reasons, and then submitted back to the industry with the assessments necessary for everybody to understand the implications of them.

I think our concern that I identified in our testimony is that we don't want to disrupt that system as a consequence of building analogous programs for other sectors. What we would like to do is share our experience with anyone who is interested to help them understand what works for us. It may not work as effectively for

other sectors. But we don't want to disrupt what we have already accomplished. Beyond that, I think we are more than pleased with what is going on today, and we simply want to continue that. Thank you.

[The statement of Mr. Meenan follows:]

PREPARED STATEMENT OF JOHN M. MEENAN

Madam Chairman and members of the subcommittee let me begin by thanking you for the opportunity to appear today. On behalf of our airline members, I would note at the outset that the focus of this subcommittee on information sharing and the associated application of analytical tools to understanding, managing and mitigating the risks of terrorism, is of paramount importance. The Air Transport Association and our member airlines are committed to providing you with our full support.

With specific reference to the subject of today's hearing—the sharing of critical homeland security information—I am pleased to report that from the perspective of the airline industry, that system is working very effectively and efficiently. Over the past six years since 9/11, the relationships, lines of communication, timeliness, quality and mutuality of the information exchange between government and industry has developed very positively. While we fully appreciate the principle behind the development of a more structured Homeland Security Information Network (HSIN), we are very concerned that, in doing so, we do not in any way inhibit or interfere with the effective system we rely upon today.

The relationship between the airline industry, the Transportation Security Administration (TSA), the Department of Homeland Security (DHS) and the broader law enforcement and intelligence communities is, of course, significantly more developed than that of other sectors. For some forty years we have been the subject of federal government regulation and direction relating to aviation security matters. Since 9/11, and with the establishment of both TSA and DHS, that relationship, of course, has reached even higher levels of sophistication.

We currently have in place well established conduits for the flow of information back and forth between industry and government. These conduits include routine reporting, telephone and electronic exchanges of information, the posting of Sensitive Security Information (SSI) on a TSA secure Web board, and classified briefings to the industry on a regular basis, as well as "need to know" briefings on developing situations. In addition, airline-specific information is conveyed through direct, secure communication (STU calls), as well as through local security briefings.

The Security Directive system and emergency program changes are communicated electronically to provide real-time updates resulting from actionable intelligence. Joint DHS and Federal Bureau of Investigation reports are provided to the industry as deemed necessary along with Homeland Infrastructure Threat and Risk Assessment Center reports. Finally, of course, the airlines are the only sector we are aware of that is required to provide TSA, are with reports of suspicious activity. These reports, once scrutinized, analyzed and processed by TSA then returned to the industry in the form of weekly suspicious incident reports.

In sum, the system we have in place is highly developed and specialized to accommodate the unique relationship between the airline industry and the responsible government authorities. We appreciate the importance of developing analogous systems for other sectors, and would welcome the opportunity to share our experience. We would, however, caution against any well intentioned but misguided effort to conform this specialized aviation system with a "one size fits all" approach applicable to all critical infrastructure sectors. We would be very concerned with requirements, through HSIN or in other ways, for duplicative, unnecessary or extraneous reporting—or any requirements that either slow the flow of information or inhibit the candid exchanges that are the hallmarks of our existing system.

Our government's approach to civil aviation security is multilayered. This is the most sensible response to the shifting threats that our nation confronts. An integral element of that approach is the government's collection and analysis of passenger information for both domestic and international flights. Vetting passengers against government watch lists—in accordance with strict procedures that recognize that such lists need to be carefully "scrubbed"—safeguards customer privacy and provides redress opportunities, substantially enhancing security for passengers and crew members alike.

These information-centric passenger vetting programs are expanding—both here and overseas. They will create substantial new demands on governmental agencies, airlines and travelers. The problem is that these governmental passenger-informa-

tion requirements, thus far, have only produced a mosaic. It remains to be seen if a coherent a picture will emerge.

Given the security threats confronting civil aviation, there is no reason to believe that that the government's passenger-information needs will abate. Passenger data will be required for the Secure Flight Program and is currently required for CBP's Advance Passenger Information System and CBP's passenger reservation information access program. Moreover, foreign governments are imposing similar demands on airlines flying to their countries, including U.S. air carriers. This unmistakable international trend is most evident with the ever increasing number of countries that require APIS information but also is reflected in the Canadian requirement for access to passenger reservation information for international flights bound for Canada, including flights from the United States. Finally, the Centers for Disease Control has proposed a rule that would require that airlines collect and store broad new categories of passenger contact information.

Information management is precisely where the government should be able to achieve a coherent policy. The continued absence of a comprehensive, government-wide passenger information access policy is a matter of real concern to us. Nor is there any indication that any element of the federal government is inclined to assume the responsibility to develop and oversee such a comprehensive policy.

This needs to change quickly. The U.S. government must produce a uniform passenger-information collection policy that applies to all of its civil aviation security and facilitation programs. Our government should also lead an effort to create such a policy for worldwide application.

A uniform policy is indispensable to the efficient collection, retention and use of passenger-information. Multiple, uncoordinated information demands do not advance aviation security. Instead, they create unneeded complexity, wasteful duplication and unjustifiable costs to the government, customers and airlines.

In conclusion, I would reiterate that from the perspective of the airline industry, we believe that our highly evolved information-sharing system is working very efficiently and effectively. Given the extensive experience that has gone into its development, we believe it could well serve as a guide to facilitate appropriate sharing by other sectors. We look forward to continuing to adjust and fine-tune our system in close consultation with our TSA and DHS counterparts. We would, however, caution strongly against any program that seeks to force changes in this highly functional system simply for the sake of cross-sectoral consistency. At the same time, with respect to the collection of passenger data as opposed to the sharing of intelligence or suspicious incident reporting, we believe that better coordination between government agencies is imperative.

Thank you very much for the opportunity to express our views on this important matter.

Mr. CARNEY. Thank you, Mr. Meenan.

Mr. Hovel for 5 minutes, please.

STATEMENT OF RICHARD E. HOVEL, SENIOR AVIATION AND HOMELAND SECURITY ADVISOR, THE BOEING COMPANY

Mr. HOVEL. Congressman Carney, Ranking Member Reichert, Congressman Dicks, it is a pleasure to be able to once again testify before this subcommittee on a topic that is so vital to industry. I had the honor of appearing before this subcommittee at your field hearing in Seattle just last May. As has been stated, I have over 35 years of cumulative law enforcement and aviation security experience, and I would like to mention including working closely with, among the subcommittee members, Congressman Reichert when he was sheriff of King County, Washington.

We at Boeing are glad that we are having this hearing. We believe it is essential for the collective security of this Nation and the public and private sector to work together and share information we have about threats to our infrastructure, and I would like to highlight simply three this morning.

One, the critical need for the fusion center partnership. This partnership is a multi-agency platform used by the government and the private sector to share vital threat information that could

affect critical infrastructure here in the United States and abroad. In working together, it is vital that the public and private sector establish a bottom-up approach by integrating not only the information sharing requirements of industry but also the vast amount of information that industry can provide.

For example, Boeing is a key producer of aerospace and defense products that are an important part of our economy. Given some of the products we make, we know we are a target for terrorist elements that would like to disrupt our ability to provide these products to our commercial customers as well as to the U.S. Government. The fusion center allows us to work with Federal, State, local law enforcement to identify potential threats to our facilities, assets and operations. For the safety and well-being of our company, many other companies and the Nation, it is essential that we continue the cooperation the fusion center has generated.

Secondly, the private sector is acutely aware of the interdependencies and preparedness gaps that lie within the various elements of the critical infrastructure. But because of the complex nature of each of these elements as well as their interdependencies, it is vital that we have access to as much information as early as possible, both classified and unclassified.

As my good friend the honorable Congressman Reichert well knows from his exemplary career in law enforcement, it is essential to have all the information available in dealing with the criminal element, which for the very same reasons is equally essential to the private sector. That is the information beyond what might be threat-specific, indicative of a long-term threat, or tactics and methods utilized by our adversaries.

Third, we would like to thank Congress for passing the Critical Infrastructure Information Act of 2002. In addition, we are pleased with the final rule issued by the Department of Homeland Security on procedures for handling critical infrastructure information and the protection of it on September 1, 2006, in response to that very act. This law encourages the private sector to voluntarily share security-related information about critical infrastructure and by providing special protection for that information.

Going forward, it is extremely important for the public and private sectors to work together to protect our national security, economy, and public welfare. Similarly, passage of the Safety Act of 2002 is an essential enabler for participation and information exchange. This gives providers of anti-terrorism technology and services a system of risk management that limits potential legal liability. Without this protection, the private sector could not participate in this activity.

Again, I thank you and certainly stand ready to answer any questions you might have.

[The statement of Mr. Hovel follows:]

PREPARED STATEMENT OF RICHARD E. HOVEL

The US Department of Homeland Security has defined the concept of a fusion center as a collaborative effort of two or more agencies that provide resources, expertise, and/or information to the center with the goal of maximizing the ability to detect, prevent, and respond to criminal, terrorist and other activity as affects our Critical Infrastructure Key Resources (CI/KR). To meet this challenge, fusion centers are evolving to an **all-threats, all-crimes, all-hazards** approach. Their in-

tended function is to compile, blend, analyze, and disseminate information of various types such as Criminal Intelligence, Threat Assessments, Public Safety, Law Enforcement, Public Health and Social Services, to name a few. To establish this successfully, a "bottom up" approach is necessary, integrating information requirements of the private sector to form the program foundation. Once accomplished, measurable progress will be dependent upon mutually understood expectations, capitalizing on already-existing relationships between the public and private sector partners.

According to the recently released National Intelligence Estimate (NIE), the ability to detect broader and more diverse terrorist plots in our current environment is certain to challenge existing US defensive efforts, as well as the tools we use to detect and disrupt these plots. To meet this challenge will require a greater understanding of how suspect activities at the local level relate to strategic threat information, and how best to identify indicators of terrorist and other criminal activity in the midst of legitimate interactions. The private sector can offer fusion centers a variety of resources, including industry-specific subject-matter experts who can provide expertise when threats have been identified. This could include information pertinent to cyber crimes, risk assessments, suspicious incidents and activities, as well as information relative to the location of CI/KR. However, understanding and responding to the myriad of CI/KR **interdependencies** as well as **preparedness gaps** that exist between them, depends upon having the latest and most complete information available. Similarly, success in the public sector in these extremely sensitive areas is predicated on a thorough understanding of the far-reaching damage that a successful attack on CI/KR could have. Industry, as a whole, is acutely aware of the vital role one element may have in the successful continuity of operations of other elements. Because of the difference and complex nature of each element of the CI, as well as their already stated interdependencies, access to **all information both *classified* and *unclassified***, which potentially or actually threatens them, is vital.

One of the fundamental principals of fusion center partners should be the identification and sharing of terrorism-related leads, that is, any **nexus** between crime-related and other information collected by state, local, tribal and private sector entities suggesting the presence of a terrorist organization and/or likelihood of an attack. A clear understanding of the links between terrorism-related *intelligence* and terrorism-related *information,* e.g. flight training school, drug trafficking, etc, must be understood so as to identify those activities or events that are precursors or indicators of an emerging threat. It is essential that a partnership between public and private sector officials be solidified, so public sector representatives may become much more familiar with prevailing vulnerabilities and consequences in the private sector, of possible terrorist attacks. Likewise, the private sector must be better educated to the methods likely utilized by terrorist organizations, and the equipment and substances needed/used to carry out an attack with associated planning activities. An outreach to non-government experts in academia and the Private sector can also add the advantage of alternative analyses and new analytic tools to broaden and deepen the intelligence community's perspective.

Other information necessary, both classified and unclassified that is vital to the private sector is that which is **threat-specific, indicative of a long-term threat and tactics and methods** used by terrorist organizations to perpetrate an attack. One objective is the production of value-added intelligence products than can support the development of performance-driven, risk-based prevention, response and consequence management programs that will support specific protective measures to identify and disrupt potential terrorist attacks during the planning and early operational stages. Benefits of this will be realized in the improved flow of information from a *common operating picture,* which supports private sector *resiliency* while satisfying public sector *mission requirements.* More specific information needs attendant to individual elements of the CI/KR may best be the product of Key Resource Sector Councils, the American Society for Industrial Security (ASIS) or other OSAC-like groups that can speak to the more in-depth characteristics of each element.

On a related note, Boeing would like to thank Congress for passing the Critical Infrastructure Information Act of 2002. We are also pleased with the Final Rule issued by the Department of Homeland Security (DHS) on Procedures for Handling Critical Infrastructure Information, on September 1, 2006, in response to that Act.

This law encourages the private sector to voluntarily share security-related information about critical infrastructure by providing special protection for that information. Going forward it is extremely important for the public and private sector to work together to protect our national security, economy, and public welfare.

The type of information that Boeing provides includes assessment of the vulnerabilities of our aviation infrastructure, which includes our airplanes. Boeing believes that this information and the thorough risk management analysis that TSA and Boeing are working on with others in government and industry are critical to improving security, safety and efficiency in U.S. commercial aviation. The U.S. aviation infrastructure remains a potential target for future terrorist strikes and the government and private sector need to keep a collective watchful eye. The PCII protections are essential to this work.

According to the NIE, Al-Qa'ida's homeland plotting is likely to continue to focus on prominent political, economic and infrastructure targets with the goals of producing mass casualties, visually dramatic destruction, significant economic aftershocks and/or fear among the US population. It goes without saying that Al-Qa'ida will continue to try to acquire and employ weapons of mass destruction (WMD) and would not hesitate to use them if it develops what it deems is sufficient capability. There are increasingly aggressive internet sites espousing anti-US rhetoric and actions, and a growing number of radical, self-generating cells in Western countries, indicating that the radical and violent segment of the West's Muslim population is expanding within the US. Other non-Muslim terrorist groups will also most likely conduct attacks over the next three years given their violent histories. To date, the bulk of the deadly attacks experienced, have been directed toward the private and quasi-private sectors. The loss of lives and damage to property suffered both domestically and overseas has been astronomical, giving companies a vested interest in joining in the fight. Currently, the resources of the private sector are hardly being tapped. Instead for the most part, businesses are (still) sitting on the sidelines relying on the US government for protection. This not only weakens our ability to eliminate terrorism, but it overlooks the fact that this is a shared problem that involves us all. The chance of winning the fight against terrorism exists, but we all need to contribute to the solution—a solution that necessitates expansion of the intelligence gathering role beyond its limits to date, and overcoming the crippling attitude that this menacing threat is the responsibility of the government alone.

Mr. CARNEY. Thank you, Mr. Hovel. And I would like to thank the panel for their testimony. I will now recognize myself for 5 minutes or so for questions, and we will continue the questions with the rest of the panel.

My first question is, Mr. Johnson, on the timeliness issue. How from your perspective do we fix it? What needs to happen to improve the timeliness?

Mr. JOHNSON. Well, I think on several fronts. One is that I think we are moving in the right direction to determine what information each of these sectors needs to receive. But the other is, is that we have to develop an atmosphere where that when there is an incident, whether it is domestic or international, when this occurs, that that information regardless of how well we have been able to go back and ensure that it is accurate and that those things take time, from our standpoint we are looking for a remediation plan. Do I need to step up protection if there are some things that I need to take place now to ensure that that doesn't happen to any of our infrastructure? So speaking at it from that standpoint, the quicker we have that information that is pushed to us that we are not relegated of calling a phone number to find out information about, but we all have numerous devices now that connect us to information. And by pushing that information out versus putting it there for us to come find it I think is the one change that I think would benefit us greatly, is that we get notified of the incident that there be continual updates providing information.

As that analytical part goes on, if they determine that the information is not accurate, what is going out on the open source areas and they can provide that to us, that too is of utmost benefit, but waiting to do that until they have had an opportunity to assess it often puts us in a position that we are having to make decisions

about whether we are expending more moneys to protect certain infrastructure or whether we are not. And obviously we need notification of those issues as quickly as we can.

Mr. CARNEY. Let me ask you from this perspective then, does SCANA, for example, have somebody or an office that monitors the Web sites that sees what is being pushed out?

Mr. JOHNSON. We do. We have individuals that we have that go to that. Primarily our quickest asset that we have found of discovering of breaking news and information is the cable news networks. That is where we find things out and we are then relegated to find our contacts within the various communities of interest and different areas of homeland and Federal and State law enforcement.

Our fusion center is a huge assistance to us, but they currently are not 24/7. When they are there, we get good notification. But they too are trying to find a methodology by which they are going to get pushed out.

Mr. DICKS. If you will just yield briefly on that point for a second.

Mr. JOHNSON. Yes, sir.

Mr. DICKS. Does your fusion center have Federal officials in it? Or is that a State fusion center?

Mr. JOHNSON. The implementation is, this summer, of a DHS official present in our fusion center. That is very new and recent.

Mr. DICKS. Is the FBI there, other Federal agencies?

Mr. JOHNSON. There is a Federal figure, they call the—the actual intelligence group has a representative there as well. Yes, sir.

Mr. DICKS. Thank you, Mr. Chairman.

Mr. CARNEY. Thank you. You will be happy to know that, for example, over at the Pentagon they also have CNN on and FOX News too.

Mr. JOHNSON. I am sure they do.

Mr. CARNEY. This is for everyone. How much information do you push up?

Mr. JOHNSON. I can speak to ours. Any incident that we have of suspicious activity around any of our facilities that have critical infrastructure, as it has been deemed critical by our assessment, we push that information to our fusion center. Certainly we have plans in place that should we have any kind of an obvious sabotage or an attack, Federal law enforcement is notified along with our State homeland security and law enforcement officials and the Department of Homeland Security would be notified in that respect as well should that occur.

Mr. CARNEY. Mr. Meenan.

Mr. MEENAN. From the airlines' perspective, we are actually under regulation required to report suspicious incidents, not that we wouldn't do that anyway. It really becomes a matter of making sure that what we are reporting is significant, is important enough to—I mean, you have to sort through these things. You can't so overburden the system with every anomaly that you end up losing any perspective on what you are reporting. So I would say we have struck a good balance at this point. We are very satisfied.

Mr. CARNEY. I will get right to you, Mr. Hovel. But along that same vein, when we see blocks of cheese with wires wrapped around them going through airports, is that considered not anomalous or how—

Mr. MEENAN. That I think is a good example of a report that draws a lot of public attention that is more in the nature of a routine report that we receive with great regularity. That is one I think TSA indicated some 90 reports of things going on. That is why it is important that the experts, the intelligence community, the law enforcement community be looking at these things to determine what is more significant and what isn't?

It is also, I think, one of the reasons that we are concerned that this information be handled with the appropriate amount of discretion as well.

Mr. CARNEY. Mr. Hovel.

Mr. HOVEL. Similarly, we too are governed by the requirements to run the information by the Department of Defense. But aside from that, we are in a little bit different situation in that my office is unique in the sense that it represents both the classified side of the house to Department of Defense as well as the commercial side. Consequently, my office deals with all matters of counterintelligence, counterespionage and counterterrorism, all three of those, which you can see quickly and easily are obviously all driven by information.

So it is extremely vital to us to have the same information as early as possible without waiting for it to be vetted as to whether it is even actionable or not. Consequently, we do report incidents that take place up to the various chains both on the defense side and on the commercial side to the levels and in the verbiage where it is appropriate to the audience, where it is warranted. But it also gives us the opportunity to analyze that intelligence ourselves with respect to our own operations to determine the relevancy.

Mr. CARNEY. Thank you. I now recognize the subcommittee's ranking member, Mr. Reichert.

Mr. REICHERT. Thank you, Mr. Chairman. Welcome to all of you. Mr. Hovel, nice to see you again. I wanted to touch on—Mr. Meenan, you suggested that the airline industry is having success in communicating with the Federal Government. What do you think that success is due to?

Mr. MEENAN. I think it is due to—fundamentally it is due to relationships. I mean from the very start of TSA's activity and indeed under its predecessor functions over at the FAA, we have a lot of personal relationships, a lot of solid business relationships that have grown into the kind of communication that I think is critical to developing the right flow between the industry and government. Those are obviously supplemented at this point with a wide array of support that has come, as you heard from the first panel, from other government agencies and entities, and the mechanisms to do it. We have got the electronic communications capability, everything from you know routine e-mails to there was a classified Web site with sensitive security information that is available to our folks. It is a very comprehensive system, and it is I think at this point quite productive. It improves daily, and we want to continue to improve it.

Mr. REICHERT. It sounds kind of simple. Build a relationship, build some trust, and then you build a system to share the information.

Mr. MEENAN. It has worked that way for us.

Mr. REICHERT. So in this process, where do you get your information from? Is it from TSA?

Mr. MEENAN. Primarily from TSA. But we also receive routine reports, high track reports, we receive FBI briefings, we receive from a variety of different sources of information. But our principal focus obviously for the airline industry is with TSA.

Mr. REICHERT. Have any members of the panel identified any chokepoints in sharing information back and forth? I know the question has already been asked about timely. But if it is not timely, why isn't it timely? Where is the roadblock if there is one?

Mr. HOVEL. Congressman Reichert, it is a chokepoint for us where we find that information is not passed along to us because of one or another reasons. One, it is possibly not deemed as actionable. Second of all, and most importantly, it may well not be understood by those who are evaluating the information, and that leads back to my previous comments concerning the interdependencies. Because of the intricate nature of each of the elements of the critical infrastructure and their significant interdependencies upon each other, it is vital that we be able to get as much information as quickly as possible to look at that information relative to these various elements. Then and only then are we going to be able to analyze it to see what implication, what relevancy it might have as well as what dangers it might pose.

Aside from that, other information that we get is coming to us in a timely manner.

Mr. REICHERT. Is the fusion center a benefit for your—and I know you have recently become a member.

Mr. HOVEL. Yes, it certainly has. In fact, sitting behind me is a gentleman that is our intelligence analyst that is assigned to the fusion center.

Mr. REICHERT. I have no further questions. Thank you.

Mr. CARNEY. Thank you, Mr. Reichert. The Chair now recognizes the gentleman from Washington, Mr. Dicks.

Mr. DICKS. Mr. Meenan, one thing that has troubled me, maybe you can help me on this and maybe you can't, one of the issues that, you know, we talk about this relationship with TSA and we have airplanes flying to the United States. One of the problems has been getting the names checked before the airplanes take off. Can you explain that to us? That seems to me to be one of those things that we have just got to fix. And is it being fixed?

Mr. MEENAN. It is being worked on every day. Actually, the names are checked before the airplanes take off. The information is exchanged. In my prepared remarks, I mentioned it is an area of difficulty for us because unlike on the intelligence and information sharing side of things, the industry is hit with multiple different requests from various government agencies for data elements about our passengers, our customers. There is very little effective coordination between all of the government agencies involved there, and it is a matter then of trying to satisfy multiple different masters.

We have urged the Department of Homeland Security to work across the government to try to minimize the duplication that is going on, make it as streamlined as possible, agree on what the data elements are, and let us build a system once and for all that

works to supply all these agencies with what they need, rather than these pop-ups that we are dealing with today.

Mr. DICKS. And that still hasn't happened?

Mr. MEENAN. It has not happened at this point. But I will say people are trying to address it. It is a very complicated set of information involved.

Mr. DICKS. Do you have any time frame on which you think this will get resolved?

Mr. MEENAN. Not at this point. But it is being addressed every day. There are, as I say, levels of complication to it. We will be happy to come by and brief you in more detail on it, but it is something that we are working on, and I think the government is working on as well.

Mr. DICKS. One area of concern to the Congress has been the fact that we go through all this complicated procedure to check all the passengers, but we don't do it with the workers at the facility. What is your take on that? Or we don't do it to the same extent.

Mr. MEENAN. I think that is something of a misinterpretation. We actually know a lot about the workers. We do a lot of checking of the workers. But what we are concerned about is there is talk, there is discussion about 100 percent screening, for example, of employees moving to and from secure areas at the airport. Many of those are the pilots who fly the airplanes, who we trust to fly the airplanes. We don't know that that is an effective and efficient use of government resources to screen them to make sure that, you know—we want them to be fundamentally screened. But there are limits to what should be done. Same thing with mechanics, people who are bringing tools onto airplanes. You know, we let them do that, and yet we are saying they need to pass through a checkpoint on the back side of the airplane to go to work. There again, some practicalities associated with that that we think just need to be thought about very carefully.

Mr. DICKS. Well, as someone who has been on this committee for a number of years, and you look at what the consequences of 9/11 were economically to the country and what we have had to do in order to try to better secure the country, I mean the ramifications of this are just immense, especially for the airline industry and for Boeing, who was adversely affected when their customers can't buy airplanes because people have stopped traveling. It is a major, major problem, and one that has concerned us. And we want to try to work with Homeland Security to improve this process.

And again, I think when we have these hearings we should have the private sector people first and get all the issues. Mr. Chairman, I know it wasn't your decision. And then bring the government witnesses up so that they can have the benefit of having heard the people from the private sector first. But I think as you have suggested, all of you, that this is a work in progress. And I am hopeful that we can continue by having oversight hearings which I think even the previous Congress did a good job on, had a lot of hearings which brought these issues out. And when you do that, then sometimes, most of the time the agencies will respond, because they recognize they want to do a better job. At least we hope so.

Mr. MEENAN. And if I might, it is one of the reasons we find the work of this committee so important. The key to good security is

risk analysis, understanding the risk and applying the resources as efficiently as you can to achieve the goal you are seeking. And I think that is something that we are all learning to do better over time. And it is going to continue to improve.

Mr. DICKS. You can't defend against everything. You have got to pick out the ones, the truly big possibilities where—and the airlines unfortunately represent that kind of a possibility, as we learned on 9/11 and subsequent to that, that it is something that is continuing to be a problem. So anyway, we appreciate your testimony, and we appreciate your working with the agencies to try to help them improve.

Thank you, Mr. Chairman.

Mr. CARNEY. Thank you, Mr. Dicks. I just have a couple of questions before we wrap it up today. Mr. Johnson and Mr. Hovel, does the private sector trust the government with proprietary information? I mean, is this an impediment to the relationship of information sharing? Is it a facilitator of it? Are there barriers we need to work on here?

Mr. JOHNSON. I can speak for our sectors and the peers that I have spoken with that there are still some issues. There was an incident that I outlined in my testimony that was provided to you earlier where a representative of or sector was in a meeting with some contractors. And during that conversation a document was presented that was absolutely protected and proprietary and had been provided under the PCII status, yet that document was out. Those incidents obviously make it very difficult. I think there is a desire to work with and trust the government with that information. But in some of those instances, some of that information is so crucial to our business units standpoint that there is still some—and will continue to be some concern about arbitrarily turning that document over from that standpoint.

Mr. CARNEY. Mr. Hovel.

Mr. HOVEL. We too have some concern. We have not had any problems, however, with that. We have been very, very happy with the protections afforded us by the law that has been enacted. We look very forward to putting into place the ACAMS element of Operation Archangel to feed the information into the database. We are right on the threshold of accomplishing that.

Mr. CARNEY. Okay. Again, I heard when Mr. Dicks was asking his questions the phrase "duplication of effort" again, and we assured the previous panel that that was really not happening. But it is happening from your perspective? Mr. Hovel?

Mr. HOVEL. Yes, it is happening but it is not necessarily a bad thing. Because oftimes we may not be privy to a particular channel of information that comes in. If there are multiple channels, then the law of averages is going to catch us sooner or later to be able to get that information in front of us. At the same time it is interesting to hear the different variations of interpretation of incidents too. So it is a critical thinking——

Mr. CARNEY. Well, is it interesting or perplexing?

Mr. HOVEL. It can be both. It certainly has in the past.

Mr. CARNEY. Understood.

Mr. Meenan.

Mr. MEENAN. It is something we are concerned about, but I must say I was reassured with the testimony from the first panel today that some of our concerns about the development of the HSIN network may be misplaced. We haven't been fully briefed on it. We have a meeting set I think next week and we just want to ensure that it is run as efficiently as possible.

Mr. CARNEY. Okay. Thanks. Mr. Johnson.

Mr. JOHNSON. I concur with the earlier speakers. But I will tell you I probably have more concern about not so much the duplication of efforts as it is to complete a project. We have had multiple issues, particularly with HSIN that have begun only to find that during a period of time there seems to be a lull that we are now moving in a different direction. It appears that we are constantly working to reinvent what we discussed and talked about before. And that seems to be the more duplicative part than it is duplicative efforts among the various parts of the Department.

Mr. CARNEY. Okay. I understand. I have no further questions. I will, however, recognize my good friend, Mr. Dent, from Pennsylvania for 5 minutes or so.

Mr. DENT. Thank you, Mr. Chairman. I appreciate that. And I guess my question would be to Mr. Meenan and to Mr. Hovel, especially with respect to the information that you are currently receiving or that is being made available to you from the Homeland Security Information Network, the HSIN. Are there any suggestions that you can make to DHS that would essentially help that agency provide you with more useful realtime information and intelligence? From your perspective and maybe from the association's perspective.

Mr. HOVEL. Certainly. There are some things that could be done to—one of the key factors is expediting the issuance of information in a more timely fashion. One of the problems that we have experienced in the Northwest is with what is called Northwest Warning and Alert Response Network, NWWARN. At first our network in NWWARN was attached to the greater communication platform of HSIN CI, and we found it was not robust enough. So we have consequently gone with another platform that does have the flexibility and the resiliency that is necessary to continue operating what it is that we believe and feel is necessary for at least our part of the country.

Mr. MEENAN. From the airline's perspective, I think because we have been so central to a lot of the post-9/11 activity at both DHS and TSA, our information sharing and the products we receive I think are pretty well developed and are pretty sophisticated at this point. From an industry perspective and down to the individual airline perspective, there are lots of close daily, hourly communications. And obviously we are always looking for areas to improve. But right now I think if anything, our sector could probably be more helpful to some of the others in understanding how to develop their own mechanisms rather than putting too much more input into that. It is working pretty well at this point.

Mr. JOHNSON. Mr. Congressman, I too would go back and concur with the comments provided by my colleague with Boeing. We too have had the same situation with the Southeast side of HSIN CI. There was a great deal of work, diligent work on both the Federal

Government side and the private sector side to identify these sector representatives, to vet these individuals, and to go out and market and sell that program among the various critical infrastructures, only to find that the actual platform now was not robust enough to allow us to continue on it, and now we are going down a different road where we have a spin-off from the Southeast Emergency Response Network, SERN, that we are now having to go back and try to remarket and go back to the same individuals where we have already been that we did not produce to try to encourage them to participate in yet another program. And that becomes more difficult each and every time we have to go back and do that. There is only so much commitment and trust that these individuals are going to put into their time. When you are dealing with the private sector, they are used to determining what an issue is, finding the answer and moving forward, not keep coming back and revisiting the same information again and again and again.

Mr. DENT. So are you basically suggesting that the information that you are being asked to provide to DHS creates an undue burden for your company in many cases?

Mr. JOHNSON. In circumstances, that would be correct.

Mr. DENT. Is that the sense of Boeing, too?

Mr. HOVEL. Yes, sir, that is the case.

Mr. DENT. What can we do—why don't you just elaborate on what you think we can do to make our compliance requirements less burdensome? What should we be doing?

Mr. JOHNSON. In our area what I am speaking to is not so much compliance as it is encouragement to utilize. Take this technology provided by the government to collaborate and exchange and receive information. I don't know if we have missed the ball going into it from an assessment standpoint or what the technology needs to be and exactly how much information there is. I almost come to the point that I feel we need to look for small successes instead of large failures. Let's take the low hanging fruit. It may not be 100 percent of what we need. But let's find something that we can complete and say that it is a success and then build off of that to get to where we need to be. Maybe instead of trying to take the entire tree, let's take the apple first and work our way up, may be a suggestion that I would have.

Mr. HOVEL. Congressman Dent, there is another element that factors into this as well, and the distinguished colleague from ATA was able to bring that element to light, and that is the differences that exist from ATA operating in a regulated environment from a security standpoint to, say, SCANA or the Boeing Company, which does not operate in a regulated environment. We are finding the balance of information that does get transmitted to the regulated side far and away exceeds that of what is received otherwise by us included. So just the information that is shared and the time of it that it is shared within is critical to us. But because we are not regulated, we don't get a timely response necessarily in all circumstances.

Mr. JOHNSON. Congressman, just for your benefit, we too work in a regulated area. Obviously we have nuclear as well as FERC and other things that we work within. And certainly from the compliance standpoint, the exchange and flow of information there is

much better than on the business units we have that may not be so heavily regulated. And I can speak from other sides of the private sector and other areas which do not have those compliance issues. These are the ones we keep coming back to again and again, asking them to participate and provide. It is just—that is the hard part, is to keep going back to the same individuals over and over.

Mr. CARNEY. Thank you, Mr. Dent. To continue along this course just for a moment, how do we convince them to come back? What can we do? What can the government do? What can Congress do from your perspectives to allay their fears?

Mr. JOHNSON. I can only speak from our successes that we have had in our State of South Carolina. On the State level, we have made good progress with sharing information. We have demonstrated our ability to do that among our law enforcement agencies where all of their incident reports are now shared into a common data warehouse, that they can come in for the first time and be able to query that information from other agencies. That has never existed before. We did that through the assistance of the National Law Enforcement and Corrections Technology Center Southeast, funded by the Federal Government through the National Institute of Justice, who are tremendous brokers of—an honest broker of technology for law enforcement. I think we can replicate that throughout the private sector. Getting the ability to access that assistance is something Congress can make happen that I think will assist us.

There are success stories there on the State level where we look and derive for particular intelligence and information from our fusion center to push out to the members of our private sector and the State. But it takes a great deal of effort, obviously, to do that, where the Federal Government can come in and whether they contract with someone to push this information out on a timely basis, whether it be situation awareness information, those things are all there. It may not be in the best interests of the timing of both the customers and the government for the government to take that role. We need to look at what areas we can contract out and utilize that where it benefits us, I think would be an area that we certainly ought to consider.

Mr. CARNEY. Anybody else care to comment? All right. Well, I want to thank the panel for their valuable testimony this morning. It is enlightening from both perspectives, from all perspectives. Please be aware that there is a possibility that the committee and members will have further questions that we would like a timely response to. It is not always the case, but we would like a timely response.

Hearing no further business before the subcommittee, we stand adjourned.

[Whereupon, at 11:40 a.m., the subcommittee was adjourned.]

VerDate Nov 24 2008 10:54 Aug 17, 2009 Jkt 000000 PO 00000 Frm 00050 Fmt 6633 Sfmt 6011 H:\DOCS\110-HRGS\110-62\48957.TXT HSEC PsN: DIANE