TERRORISM RISK ASSESSMENT AT THE DEPARTMENT OF HOMELAND SECURITY

HEARING

BEFORE THE

SUBCOMMITTEE ON INTELLIGENCE, INFORMATION SHARING, AND TERRORISM RISK ASSESSMENT

OF THE

COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES

ONE HUNDRED NINTH CONGRESS

FIRST SESSION

NOVEMBER 17, 2005

Serial No. 109–58

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
35–939 PDF WASHINGTON : 2007

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

COMMITTEE ON HOMELAND SECURITY

PETER T. KING, New York, *Chairman*

DON YOUNG, Alaska
LAMAR S. SMITH, Texas
CURT WELDON, Pennsylvania
CHRISTOPHER SHAYS, Connecticut
JOHN LINDER, Georgia
MARK E. SOUDER, Indiana
TOM DAVIS, Virginia
DANIEL E. LUNGREN, California
JIM GIBBONS, Nevada
ROB SIMMONS, Connecticut
MIKE ROGERS, Alabama
STEVAN PEARCE, New Mexico
KATHERINE HARRIS, Florida
BOBBY JINDAL, Louisiana
DAVE G. REICHERT, Washington
MICHAEL MCCAUL, Texas
CHARLIE DENT, Pennsylvania
GINNY BROWN-WAITE, Florida
BENNIE G. THOMPSON, Mississippi
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
BILL PASCRELL, JR., New Jersey
DONNA M. CHRISTENSEN, U.S. Virgin Islands
BOB ETHERIDGE, North Carolina
JAMES R. LANGEVIN, Rhode Island
KENDRICK B. MEEK, Florida

SUBCOMMITTEE ON INTELLIGENCE, INFORMATION SHARING, AND TERRORISM RISK ASSESSMENT

ROB SIMMONS, Connecticut, *Chairman*

CURT WELDON, Pennsylvania
MARK E. SOUDER, Indiana
DANIEL E. LUNGREN, California
JIM GIBBONS, Nevada
STEVAN PEARCE, New Mexico
BOBBY JINDAL, Louisiana
CHARLIE DENT, Pennsylvania
GINNY BROWN-WAITE, Florida
PETER T. KING, NEW YORK *(Ex Officio)*
ZOE LOFGREN, California
LORETTA SANCHEZ, California
JANE HARMAN, California
NITA M. LOWEY, New York
SHEILA JACKSON-LEE, Texas
JAMES R. LANGEVIN, Rhode Island
KENDRICK B. MEEK, Florida
BENNIE G. THOMPSON, Mississippi *(Ex Officio)*

CONTENTS

TERRORISM RISK ASSESSMENT AT THE DEPARTMENT OF HOMELAND SECURITY

Thursday, November 17, 2005

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 3:05 p.m., in Room 311, Cannon House Office Building, Hon. Rob Simmons [chairman of the subcommittee] presiding.

Present: Representatives Simmons, Lungren, Dent, Lofgren, and Thompson (ex officio).

Mr. SIMMONS. The Committee on Homeland Security Subcommittee on Intelligence, Information Sharing and Terrorism Risk Assessment, will come to order.

The subcommittee is meeting today to hear testimony on terrorism risk assessment at the Department of Homeland Security. We will be hearing testimony from four witnesses today. We will first hear from Ms. Melissa Smislova, Acting Director, Department of Homeland Security, Homeland Infrastructure Threat and Risk Analysis Center.

We will also hear from Ms. Christine Wormuth, Senior Fellow in International Security at the Center For Strategic and International Studies.

We will hear from Dr. Detlof von Winterfeldt, Director of the Center for Risk and Economic Analysis of Terrorism Events at the University of Southern California.

We will hear from Dr. Henry Willis, Policy Researcher with the RAND Corporation.

I welcome you all here today.

Preventing terrorist attacks and assuring the safety and survivability of our Nation's critical infrastructure and key resources remains at the core of the DHS mission. To accomplish this mission, it is not enough to simply develop a comprehensive understanding of what we are protecting and what it is that is important to us as a Nation. We must also complete the picture by accurately and quickly fusing that knowledge with an understanding of America's enemies and the threats we face. It is only when we are able to successfully bring these two elements together that we can accurately gauge and respond to the risks we are confronting in the war on terrorism. This challenge is at the heart of terrorism risk assessment at the Department of Homeland Security.

The Department of Homeland Security, as stated in the Homeland Security Act of 2002, is required to, "integrate relevant information, analyses and vulnerability assessments in order to identify priorities for protective and support measures by the Department, other agencies of the Federal Government, State and local agencies and authorities, the private sector and other entities." In other words, to understand the Nation's vulnerability, to understand the internal and external threats to our homeland, and to bring that information together and help ensure appropriate action is taken and policies enacted.

To more effectively carry out this critical role, the Department stood up the Homeland Infrastructure Threat and Risk Analysis Center, or HITRAC.

The Department of Homeland Security has the unenviable task of gathering vulnerability data from across the United States from a wide variety of critical infrastructures and key resources. That data must then be combined with a comprehensive consequence analysis and further coupled with the best threat information that Federal, State, local and tribal governments can provide. This is a vitally important task, and while it must be done as quickly as possible, it is also important to get it done right, putting the highest priorities first.

We look forward to hearing your views on how the Department and the risk analysis community are meeting that challenge and working to ensure the security of the homeland.

The Chair now recognizes the ranking minority member of the subcommittee, the gentlelady from California, Ms. Lofgren, for any comments she might have.

Ms. LOFGREN. Thank you, Mr. Chairman. I am glad that we are turning our attention today to the Department of Homeland Security's approaches, capabilities and plans regarding the third component of this subcommittee's oversight jurisdiction, terrorism risk assessment. This is the first time that we are addressing this risk assessment issue directly and, more specifically, the criteria the Department should consider as part of its work in this area.

If done correctly, a coordinated terrorism risk assessment will go a long way to help the Department decide where to target investments in combating terrorism, what critical infrastructure to secure and how to set priorities on the basis of risk.

Developing an effective risk assessment strategy is especially important as we acknowledge that our private sector partners now own approximately 85 percent of the critical infrastructure in this country. In order to get the private sector to buy in to what the Department is doing in this area, however, we need the Department to partner effectively to develop consistent and flexible risk assessment criteria and to create incentives to ensure private sector participation.

While I am certain that the testimony today will address all of these issues, and while this hearing is clearly an important one, I nevertheless wonder if we are not putting the cart before the horse. Most risk analysts agree that before you can do meaningful risk and threat assessment, you must first know what it is that needs protecting.

The administration began an effort to create a national database of potential terrorist targets such as dams, pipelines, chemical plants and the like, more than 2 years ago. It was supposed to use that database to prioritize assets in order of risk and to harden facilities and systems accordingly. I am sorry to report that the database is still full of holes and has not been finished.

Because the Department lacks the methodology to rank critical assets contained in the database, incomplete as it is, the Department to date has essentially assembled a spreadsheet of targets that, for the most part, does not tell the Department or Congress what to protect first or why.

Part of the problem stems from the Department's failure at the outset of the database project to set clear standards for which assets should and should not be considered critical for homeland security purposes. Indeed, this lack of standards resulted in a miniature golf course in my home district being included as a critical homeland security asset. This would be funny if the stakes were not so high. Without standards, how that miniature golf course ranks in priority against protecting the Capitol building or a chemical facility or subway system remains an important question that the Department can't answer.

I am dismayed that as of late last week the Department still had not submitted a report on its progress in completing, first, risk and vulnerability assessments of the Nation's critical infrastructure; secondly, the accuracy of the government's plans to protect such infrastructure; and finally, the government's readiness to respond to threats against the United States. Pursuant to the Intelligence Reform Act, that report was due this past June.

I look forward to hearing about HITRAC and how the Department might consider assessing risk on a going forward basis. I am also particularly interested in what the risk assessment experts with us today have to say about how the Department should do this important work and how effective terrorism risk assessment can really be without a prioritized dynamic list of critical assets to guide the Department's efforts.

I look forward to your testimony, and I welcome your participation in this hearing.

Thank you, Mr. Chairman.

Mr. SIMMONS. I thank the ranking member.

The Chair recognizes the ranking member of the full committee, the gentleman from Mississippi, Mr. Thompson, for any statement he may wish to make.

Mr. THOMPSON. Thank you very much, Mr. Chairman. I look forward to the testimony of the witnesses for the hearing today. I have a written statement, and I will submit it for the record. Thank you.

[The statement of Mr. Thompson follows:]

PREPARED OPENING STATEMENT OF HON. BENNIE G. THOMPSON

- I am very pleased that this Subcommittee is addressing the issue of how the Department conducts terrorism risk assessments.
- This function is critical to driving informed decisions about where to spend our homeland security dollars to protect our people, to secure our critical infrastructure, and—hopefully—to thwart terrorist attacks.

• I am very pleased that we have with us today a representative from HITRAC ("High-Track")—the Department's Homeland Infrastructure Threat and Risk Analysis Center.
• Since it was created in January of this year, HITRAC has fused the talents of both intelligence analysts and infrastructure protection experts within the Department in order to separate the wheat from the chaff when it comes to terrorist risks and threats.
• I note that in many ways, HITRAC embodies what Congress had hoped the Information Analysis and Infrastructure Protection Directorate would be—a center for intelligence analysis and risk assessment devoted to protecting and securing the homeland.
• I sincerely hope that HITRAC can efficiently do what IAIP apparently could not, and I am interested in hearing about what lessons HITRAC has learned from the IAIP experience.
• This hearing, moreover, could not be more timely. On November 2nd, the Department finally released its draft National Infrastructure Protection Plan—which I note HITRAC's operations will support once the NIPP is finalized next year.
• Among its provisions, the draft NIPP addresses the need for a common approach to assess risk in order to set protection priorities.
• The draft NIPP likewise references the RAMCAP—a series of terrorist risk assessment tools that the Department is presently developing. Unfortunately, the draft NIPP is short on details about what criteria should apply to ensure effective assessments.
• It appears, however, that the Department may face significant hurdles in obtaining RAMCAP participation.
• Some in the private sector have complained that the Department has offered few incentives to the private sector for RAMCAP participation.
• Compliance with RAMCAP methodologies, moreover, is purely voluntary.
• And according to the NIPP, the Department is planning to create multiple versions of the RAMCAP applicable to different sectors—rather than a single, flexible standard.
• I look forward to hearing all of the witness' views of the draft NIPP and the RAMCAP generally, as well as suggestions for improving upon the Department's risk assessment approach on a going forward basis.
• Thank you for joining us today.

Mr. SIMMONS. I thank the gentleman.

I notice we also have the gentleman from California here today, Mr. Lofgren. As is our custom, you are free to insert any statements you may wish for the record.

Mr. LUNGREN. I am Mr. Lungren.

Ms. LOFGREN. He is my cousin, not my brother.

Mr. LUNGREN. Tomato, tomato, and I notice it is HITRAC, and as Ms. Lofgren and I both call it, HITRAC, because I think we were both English majors in college.

Mr. SIMMONS. I thank the gentleman for his correction.

The Chair now calls our panel of witnesses. What I will do is read a short bio for each witness before they make their statement. That way it will be fresh in our minds, their background and their experience. I will advise the witnesses that we do have their full statement in the record which we can read and follow. If they wish to summarize we will be providing 5 minutes for their statements, at which point we will then ask questions.

Our first witness is Ms. Melissa Smislova, currently serving as Acting Director of the Homeland Infrastructure Threat and Risk Analysis Center. I call it HITRAC. I kind of like that better. It may be HITRAC. Maybe you can answer that question when you begin.

Prior to joining DHS, she spent almost 20 years in the field of intelligence analysis, most recently at the Defense Intelligence Agency. She brings a wealth of intelligence and analytical experience to her current role, which will serve the Department of Home-

land Security and HITRAC well as they work to fulfill the critical mission of protecting our homeland from terrorist attack.

I thank you for being here today. Please begin your testimony.

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

Ms. SMISLOVA. Good afternoon, Mr. Chairman, and distinguished members of this committee. Thank you for having me here today to speak with you about the role of the Office of Intelligence and Analysis in the development of the DHS risk assessment process.

As Secretary Chertoff has reinforced, DHS has adopted a risk-based approach in both our operations and in our philosophy. Because intelligence is a key component of risk analysis, the Office of Intelligence and Analysis, as well as the Office of Infrastructure Protection, did establish the Homeland Infrastructure Threat and Risk Analysis Center, which we do call HITRAC. HITRAC is meant to—

Mr. SIMMONS. Boy, what a terrific witness we have.

Ms. SMISLOVA. Thank you, sir.

HITRAC is meant to institutionalize risk assessments, as well as to produce some tailored threat assessments that can support the protection of the national critical infrastructure and our key resources. HITRAC reports both to the Office of Intelligence and Analysis, as well as to the Office of Infrastructure Protection, and we are comprised of members that belong to both groups.

Under this dual structure, the priority of our infrastructure work requirements does come from the Office of Infrastructure Protection under the Assistant Secretary, Robert Stephan, but the approval of all the intelligence-derived production does remain with Mr. Charlie Allen, the new Assistant Secretary for Intelligence and Analysis.

The HITRAC mission represents a unique capability within the U.S. Government. Our threat analysts have access to traditional Intelligence Community reporting and the data, as well as to the DHS component intelligence and information reporting. Our HITRAC infrastructure protection sector specialists, on the other hand, who possess the private sector expertise and sector-specific incident data, identify the sector-specific vulnerabilities and the consequences of a possible terrorist attack. Our HITRAC analysts then integrate all of this available information into strategic level risk assessments for the Federal, State and local authorities, as well as the private sector.

In addition, we believe that our intelligence products are more relevant to infrastructure owners and operators because we frame our analysis in the context and unique operating environment of our diverse and specific critical infrastructure partners.

We receive information about United States critical infrastructure through our Information Sharing and Analysis Centers, the ISACs, as well as through our contacts through the private and public infrastructure owners that have already been established by our colleagues in the Office of Infrastructure Protection and throughout the Preparedness Directorate.

In addition, we are able to refine our national level Intelligence Community collection requirements by working back through the Office of Intelligence.

DHS defines risk as the determination of weighting the factors of threat, vulnerability and consequence. While inherently the most subjective component of this risk equation, the threat of the enemy attack is derived from a study of enemy intent and capability. The intent of this particular adversary is assessed after study of all available information that we have about what this adversary wants to accomplish by attacking the United States. We work with our partners in the Intelligence Community to understand as much as we are able about the terrorists' goals, plans and desires.

We match what we know about the intentions of this adversary with information that we do have about how this enemy is capable of accomplishing an attack. For this part of the equation, we rely both on what we see the enemy discussing, recruiting and training, as well as the lessons that we are learning from his attacks overseas.

We work all the pieces of this puzzle together. HITRAC's unique partnering with the infrastructure protection specialists that are not professional intelligence officers allows us a different view of the data than what we believe our Intelligence Community colleagues sometimes have.

One example of the integration of how Department of Homeland Security integrates threat analysis into our risk assessments is shown in our HITRAC production plan to support the National Infrastructure Protection Plan. Directed by the Homeland Security Presidential Directive 7, the National Infrastructure Protection Plan is a unified national plan for the consolidation of critical infrastructure protection activities. We call that the NIPP.

The NIPP is a collaborative effort between the private sector, State, local, territorial and tribal entities and all relevant departments and agencies of our government. The cornerstone of the National Infrastructure Protection Plan, the NIPP, is a risk management framework that combines threat, vulnerability and consequence information.

Mr. SIMMONS. If you want to summarize? I have actually read your statement. I am sure we all have.

Ms. SMISLOVA. Yes. That is just why we have established a HITRAC, to accomplish those specific tasks. Thank you.

[The statement of Ms. Smislova follows:]

PREPARED STATEMENT OF MELISSA SMISLOVA

Introduction

Good afternoon, Mr. Chairman and distinguished Members of this Committee. I am here to speak with you about the role of the Office of Intelligence & Analysis in the development of DHS risk assessments.

As Secretary Chertoff has reinforced throughout his tenure, DHS has adopted a risk-based approach in both our operations and our philosophy. There is no question that intelligence is a key component of risk analysis. For this reason, the Office of Intelligence & Analysis and the Office of Infrastructure Protection established the Homeland Infrastructure Threat and Risk Analysis Center (HITRAC) to institutionalize strategic risk assessments and produce tailored threat documents in support of the protection of national critical infrastructure and key resources (CI/KR).

Homeland Infrastructure and Risk Analysis Center

The Homeland Infrastructure Threat and Risk Analysis Center (HITRAC) reports to both the Office of Intelligence Analysis (OI & A) and the Office of Infrastructure Protection (OIP). It brings together members of the Intelligence Community under OI & A and infrastructure specialists from the OIP as well as experts from the National Communications System and the National Cyber Security Division, among others, to produce strategic-level risk assessments. Under this dual structure, priority of infrastructure work requirements come from the Assistant Secretary for Infrastructure Protection, Mr. Robert Stephan, while approval for all intelligence derived production remains with the Assistant Secretary for Intelligence and Analysis, Mr. Charlie Allen.

The HITRAC mission represents a unique capability within the U.S. Government. HITRAC threat analysts have access to traditional intelligence community reporting and data as well as to DHS component-specific intelligence and information reporting (for example, information gathered at the ports of entry and transportation centers by DHS component members). HITRAC infrastructure protection sector specialists, who possess private sector expertise and sector specific incident data, identify sector-specific vulnerabilities and consequences of attack. HITRAC analysts then integrate all available information to produce strategic-level risk assessments for Federal, State and local authorities and the private sector.

HITRAC crafts products that make intelligence information more relevant to infrastructure owners and operators by framing our analysis in the context and unique operating environment of all seventeen CI/KR sectors. HITRAC receives information about the critical infrastructure through our Information Sharing and Analysis Centers and through contacts with private and public infrastructure owners that have been established by the OIP and throughout the Preparedness Directorate. In addition we are able to refine national intelligence community collection requirements though working with OI&A.

In addition, HITRAC produces threat products for infrastructure owners and operators to use in their own risk calculations and for DHS, state and local entities, and other Federal entities to use in their own planning and operations. DHS defines risk as a determination of weighing the factors of threat, vulnerability and consequence. While inherently the most subjective component of the risk equation, threat of enemy attack is derived from study of enemy intent and capability. Intent of this adversary is assessed after study of all available information about what they want to accomplish by attacking the United States. We work with our partners in the intelligence community to understand as much as we are able about the terrorists' goals, plans, and desires. We match what we know about the intentions of the adversary with information we have about what the enemy is capable of accomplishing. For this part of the equation we rely both on what we see the enemy discussing, recruiting and training for as well as lessons learned from overseas attacks. We work all the pieces of the information puzzle. HITRACs unique partnering with Infrastructure Protection specialists that are not professional intelligence officers allows us a different view of the data than our IC colleagues.

Threat Products Supporting the National Infrastructure Protection Plan

One example of the integration of threat analysis with DHS risk assessment efforts is in the HITRAC production plan to support the National Infrastructure Protection Plan. Directed by Homeland Security Presidential Directive 7 (HSPD–7), the National Infrastructure Protection Plan (NIPP) is a unified national plan for the consolidation of critical infrastructure protection activities. The NIPP is a collaborative effort between the private sector, State, local, territorial and tribal entities and all relevant departments and agencies of the Federal government.

The cornerstone of the NIPP is a risk management framework that combines threat, vulnerability, and consequence information to produce a comprehensive, systematic, and informed assessment of national or sector risk that drives our protection efforts in the CI/KR sectors. This framework applies to the general threat environment as well as specific threats or incident situations.

HITRAC's production plan supports the NIPP. The NIPP promises sector specific threat information to each sector following its finalization. Our analytic products are designed to provide threat information to the private and public infrastructure owners and operators. In particular we are producing:

- **Sector Assessments** for each CI/KR sector. HITRAC through the OI & A and in coordination with TSA and USCG intelligence entities will produce several sub-sector assessments due to the broad characteristics of some sectors (for example, HITRAC will produce sub-sector assessments for aviation and mass transit which are sub-sectors of the broader transportation sector). HITRAC leverages the expertise of several sector specific agencies, including the Trans-

portation Security Administration, as well as our colleagues in the intelligence community to support our efforts. These products, written at multiple classification levels, provide DHS a vehicle to deliver long-term strategic assessments of sector risks by detailing HITRAC analysis of the intentions and capabilities of known terrorists and integrating relevant threat information with the unique vulnerabilities and consequence of each sector.

• **HITRAC is also producing Common Threat Themes** in support of the NIPP and other DHS and Federal risk assessments. These threat scenarios are descriptions of potential attack methods based on known or desired terrorist capabilities. These scenarios, which will be updated as needed, are detailed vignettes of the methods terrorist might use to attack the US infrastructure and are derived from the study of terrorist intentions and capabilities. These scenarios are intended to inform vulnerability and consequence analysis while ensuring that a given risk analysis has taken into account the minimum set of potential attack vectors and the associated vulnerabilities and consequences.

These threat themes are used as the foundations to design and build the threat scenarios used by the Office of Domestic Preparedness. The scenarios used for ODP exercises are lengthy depictions of how a notional terrorist attack might unfold and they are drafted to test prevention and response capabilities. HITRAC's threat themes are specific descriptions of ways the enemy can attack and are for use by private and public infrastructure owners and state and local governments to develop their own risk assessments. For example, they describe in detail what we know about how the adversary can employ a vehicle borne improvised explosive device.

Conclusion

The Federal government and private sector owners and operators need intelligence-based risk assessments to best protect against and respond to potential terrorist attacks. DHS established HITRAC to provide integrated strategic risk assessments and tailored threat products in support of the protection of critical infrastructure and key resources throughout the nation. This is a very challenging mission, but with your support, we will succeed.

Thank you.

Mr. SIMMONS. Thank you very much.

Our next witness is Christine Wormuth, Senior Fellow in International Security at the Center for Strategic and International Studies, where she focuses on homeland security policy, U.S. national security strategy and policy and defense requirements and resource issues.

Prior to joining CSIS, she was a principal at DFI Government Services, a defense consulting firm, where she developed a methodology to assess homeland security risks, including an analytical tool that comprehensively evaluates homeland security risks in terms of their potential to occur and possible consequences. She works closely with elements of DHS and the Homeland Security Council on a wide range of implementation issues aimed at increasing the preparedness level of the United States.

Thank you for being here. You may begin.

STATEMENT OF CHRISTINE WORMUTH, SENIOR FELLOW, INTERNATIONAL SECURITY PROGRAM, CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES

Ms. WORMUTH. Thank you, Mr. Chairman, and thank you other members of the subcommittee for asking me to testify here today on this important topic.

Assessing homeland security riskS, which, of course, can come both from terrorism but also from natural disasters, is an enormously complex undertaking, but it is also, as you all know well, a critical task if the government seeks to marshal its finite resources effectively.

I think Ms. Smislova has very well covered the basic components of risk assessment, so I will try to focus my comments on some of the challenges that I think are inherent in developing risk assessments for homeland security, as well as some observations about the broader strategic role that I think risk assessments can play in this field.

The basic formula for risk assessment is simple. It is essentially probability, which is threats and vulnerabilities times the consequences of particular attacks, and that equals the risks. But in practice, I think analysts and experts face a lot of important practical challenges when they try to go about the task of assessing homeland security risks.

One challenge, of course, is the lack of quantitative data. We can't determine the probability in a scientific sense of a terrorist attack, the percentage chance that a particular type of attack might occur, nor do we have extensive quantitative data at this point on the specific economic costs or the potential numbers of fatalities or serious injuries that are associated with different types of attack. One way to compensate, of course, for these challenges is to use expert judgment and to use computer modeling and simulation to extrapolate information based on what we do know.

Another challenge I think that is important to note is how to handle intelligence in these types of assessments, and specifically by that I mean how can DHS develop models that factor in specific intelligence without skewing the assessment away from areas where we may not have specific information.

Coming out of the Defense Department, I am fond of quoting Secretary Rumsfeld, who has said we don't know what we don't know. Just because the Intelligence Community doesn't know that a terrorist group doesn't have WMD does not mean that they don't in fact have some sort of capability.

I think another policy challenge here is weighting the different pieces of a risk assessment. For example, should we weight different types of critical infrastructure targets or other critical assets more heavily in an assessment because a group like al-Qa'ida has expressed the intention to attack them, or should we weight human deaths and injuries more heavily than other elements of consequences. Those are policy decisions that I think we need to grapple with.

Despite these challenges, I heartily believe that risk assessment is a very powerful tool for homeland security policymakers and should be at the heart of our approach.

I do want to observe that I think DHS would serve not just itself as a department but the entire interagency, all of those cabinet agencies that have a role in homeland security, by taking the lead in developing what I like to call a National Homeland Security Risk Assessment.

I see this as being something like a National Intelligence Estimate in that it would be developed on a regular basis, perhaps every couple of years, and it would serve as the authoritative assessment of risk and trends of significance in the area of homeland security.

In my view, development of a National Risk Assessment should be actually an interagency undertaking, not just a DHS under-

taking, although DHS should certainly be in the lead. But I think to really develop this kind of risk assessment it would be useful to draw on the expertise and the viewpoints of the other cabinet agencies that have a role in this field.

I think a National Risk Assessment should focus on developing a strategic picture in the near term, at least in terms of setting broad priorities and directions, and then the details, all of those very important details, can be filled in over time with tools that are specifically developed to capture all of the nuances of the information.

In my view, a risk assessment of this type could strengthen our homeland security policy development process and resource allocation process in three important ways: First, in guiding Homeland Security planning. At CSI, as noted in our recently released "Beyond7 Goldwater–Nichols Phase II" report, a strategic risk assessment really needs to be at the heart of developing concepts of operation for homeland security. It should also serve I believe as the basis for developing national homeland security planning scenarios.

The 15 scenarios released by the Homeland Security Council are an important first step, but I think these scenarios would carry more weight across the interagency if they were based on a strategic risk assessment.

Of course as you know, a risk assessment is very important in driving the resource allocation process. Again, I think a strategic risk assessment could harmonize our efforts, not just in DHS, but across the entire intergency, which would go a long way towards maximizing our unity of effort.

Lastly, I think a risk assessment tool would help us evaluate the program options for mitigating consequences and enhancing our preparedness system, helping us think about where do we get our best bang for the buck.

I will just conclude by noting that in my view, as you know, Secretary Chertoff has called on Congress to approve an Under Secretary for Policy. Assistant Secretary Baker sits in that chair right now. I believe one of his central responsibilities should be taking the lead in developing this kind of National Homeland Security Risk Assessment and then institutionalizing its results into the DHS resource allocation process and policy planning process.

My colleagues at CSI have called on DHS to deliver a National Homeland Security Assessment by December 2006. I think this is still a very reasonable deadline. Obviously it would be wonderful to have more time, but I think given we are 4 years after September 11, it is very important to have a National Homeland Security Risk Assessment soon, even if it means that we as Americans, as you in Congress and our leaders in the executive branch, have to make choices based on less than perfect information. I think it is important not to let the best be the enemy of the good.

I thank you very much for the opportunity to share my views.

[The statement of Ms. Wormuth follows:]

PREPARED STATEMENT OF CHRISTINE E. WORMUTH

Mr. Chairman, Ranking Member Lofgren, members of the subcommittee, thank you for inviting me to testify before you today on assessing the risks of terrorism.

Assessing homeland security risks, which can stem from both terrorism and natural disasters, is an enormously complex undertaking but is also a critical task if the federal government seeks to marshal its finite resources effectively. Before turning to the key policy issue of how to use risk assessments to maximize unity of effort at the federal level, I would like to briefly outline what makes a basic risk assessment and some of the challenges inherent in trying to assess homeland security risks.

As Secretary Chertoff has emphasized since being named Secretary of Homeland Security, focusing on the "trio of threat, vulnerability and consequence as a general model for assessing risk" is at the heart of the DHS approach. It is worth peeling back the layers of the onion in those three areas a bit more fully to understand the complexities associated with assessing homeland security risks.

In most formal discussions of risk assessment, risk is defined as the product of the probability that a certain event might occur—a suicide bomber attack on a hotel such as we saw take place last week in Jordan—and the consequences that could result from such an event. The probability side of the equation is basically a combination of threats and vulnerabilities. Threats could be assessed in terms of the different kinds of weapons and delivery systems that might be available to our enemies. In some cases weapons could be relatively difficult to acquire or develop, like the smallpox virus or a small nuclear device, or they could be much more common—an improvised explosive device carried on a delivery truck. Assessing vulnerabilities means establishing the pool of possible targets—which could include buildings that are vulnerable every day like chemical plants or once-a-year events like the Super Bowl—and determining how vulnerable they are to the full range of threats. The final piece of a basic risk assessment involves looking at the consequences that might result from different attacks. Consequences might include not only the deaths and injuries that could result, but also the economic and psychological costs of a given type of attack, and the length of time it takes to resume normal activity levels after the attack.

The basic formula for a risk assessment is simple—probability times consequences equals risks—but in practice assessing homeland security risks poses some important practical challenges.

One challenge is the lack of quantitative data on which to base assessments of probability and consequences. We cannot determine the probability of terrorist attacks—the "percent chance" that a specific type of attack might occur. Nor do we have extensive quantitative data to pinpoint the numbers of potential fatalities or economic costs that might be associated with particular kinds of attacks. And how should we begin to think about psychological consequences? Can they be expressed quantitatively? We can use expert judgment and computer models to extrapolate representations of probability and consequences but they will be just that—representations rather than certainties.

Another challenge is how to handle intelligence. Many of you on the committee have noted the importance of intelligence in developing homeland security risk assessments. But determining how to incorporate intelligence effectively is a challenge for analysts. How can DHS develop models that factor in specific intelligence we may have about particular targets or payloads without skewing an assessment toward only those risks on which we have intelligence? As Secretary Rumsfeld has often said, "we don't know what we don't know,"—just because the intelligence community does not have information that suggests a terrorist group has a WMD capability does not mean that group doesn't have a WMD capability. Or vice versa.

Whether to weight the different pieces of a risk assessment is another challenge. Should some kinds of targets be weighted more heavily if we know groups like al-Qa'ida have expressed the intention to attack them? Should human deaths be weighted more heavily than other types of consequences? By how much?

Despite these formidable challenges, it is absolutely worth the time and effort to develop robust homeland security risk assessments that can guide our planning and policy development. Risk assessments—even if they are based on imperfect intelligence, expert opinion, and computer simulations of potential consequences—give us the tools to examine many different pieces of complex information in a structured way. They focus attention on the specific judgments that cumulate into an overall risk ranking and hence they can be "unpacked" to better understand where differences of opinion may lie and how they affect the assessment. Policy makers can use the structure that risk assessments provide to understand clearly where there are disagreements in the expert community, and can then assess for themselves the different sides of the debate before coming to a policy judgment that may have profound implications down the road.

DHS would serve all of the Cabinet agencies with homeland security responsibilities well by taking the lead in developing a "National Homeland Security Risk As-

sessment" that would assess and rank the full spectrum of plausible homeland security risks—an assessment that would look comprehensively across all of the kinds of critical infrastructure and other potential target types combined with the different weapon payloads and delivery systems that adversaries might seek to use against the United States. As this Committee knows well, the legislation that established DHS stipulated that the department would develop a comprehensive risk assessment. This assessment is still of paramount importance.

This type of assessment, much like a National Intelligence Estimate, would be developed on a regular basis, perhaps every couple of years, and would serve as the authoritative assessment of homeland security risks, identify trends of significance for homeland security and if necessary, identify differences of views about risks among the principal senior leaders in the U.S. government homeland security arena. Development of a National Risk Assessment should be an interagency undertaking, with DHS in the lead, but with significant support from the broader intelligence community, DoD, HHS, the Department of Energy, other Cabinet agencies, and leaders from the private sector and industry. A National Risk Assessment would sacrifice examining the threats, vulnerabilities and consequences of every possible scenario in their fullest details for a process that could generate actionable results in the near-term, at least in terms of setting broad priorities and directions. Subsequent, more detailed risk assessments focused on specific threats or infrastructure sectors could then fill in the details over a longer period of time.

A National Risk Assessment could strengthen the homeland security policy development and resource allocation process in at least three very important ways.

- *Guiding homeland security planning.*. As CSIS noted in its recently released *Beyond Goldwater Nichols Phase II* report, before the interagency can develop robust concepts of operations for homeland security, it needs to conduct a strategic risk assessment. A National Risk Assessment would not only serve as the basis for developing common interagency strategies for addressing specific homeland security challenges, it would also serve as the basis for developing national homeland security planning scenarios. Putting forth the fifteen Homeland Security Council scenarios was an important step toward harmonizing ongoing planning activities, but those scenarios could play a larger role in driving policy, planning, and programming if they were based on the results of an interagency-agreed National Risk Assessment.
- *Driving the resource allocation process.* Many have noted the importance of using risk assessments to set broad priorities for how DHS allocates resources. Looking beyond DHS, a National Risk Assessment could serve as the basis by which to harmonize not just DHS resource and policy decisions, but homeland security related resource and policy decisions across the entire interagency. This would go a long way toward creating maximum unity of effort across the USG in this critical area.
- *Evaluating potential policy and programmatic options.* Where should DHS and other agencies invest their marginal dollars? What will give us more bang for the buck, ten more bomb detector dog teams, 50 more handheld radiation detectors, or 100 more border patrol agents? These are the kinds of real world decisions DHS and other agencies have to grapple with in their budget processes, and risk assessment tools can help shed light on these choices in a structured way.

Secretary Chertoff has asked Congress for the authority to establish an Under Secretary for Policy in DHS. This is a very important and much needed position, and it is good news that Mr. Stewart Baker was confirmed earlier this year at the Assistant Secretary level. In my view, one of his central responsibilities should be to lead the development of a National Risk Assessment, working closely with his peers in the other relevant Cabinet agencies, and then to institutionalize the results into DHS's broader strategic planning and resource allocation processes. The Under Secretary, with his direct access to Secretary Chertoff, can elevate and integrate the many useful risk assessment processes ongoing inside DHS to help build a coherent, comprehensive risk assessment picture that truly drives policy and programming at the strategic level. In *DHS 2.0, Rethinking the Department of Homeland Security,* my colleague David Heyman at CSIS and James Carafano of the Heritage Foundation called on DHS to deliver a comprehensive risk assessment to our top national security leaders by December 2006. I think this remains a reasonable deadline. Highly granular assessments will clearly be needed, and there are assessment tools in development that will help us make finely tuned adjustments to our prevention, response and preparedness programs over time. But today, more than four years after the September 11 attacks, we need a comprehensive National Risk Assessment—and we need it soon. That means senior leaders, in the Executive branch and here in Congress, will have to make choices and set priorities on less than perfect

information. That said, I suspect most Americans would prefer to see the government make those tough choices rather than letting the best be the enemy of the good. I applaud this Committee for engaging on this issue and thank you for the opportunity to share my views.

Mr. SIMMONS. Thank you for that testimony. That will lead to some interesting questions, I am sure.

Our next witness is Dr. Detlof von Winterfeldt, who is the Director of the Center for Risk and Economic Analysis of Terrorist Events at the University of Southern California. He is also Professor of Public Policy and Management in the School of Policy Planning and Development. His research interests are in the foundation and practice of decision and risk analysis as applied to technology, environmental and security problems. He is the coauthor of two books and the author or coauthor of over 100 articles and reports on these topics.

Thank you very much for being here. We look forward to hearing your testimony.

STATEMENT OF DR. DETLOF von WINTERFELDT

Mr. VON WINTERFELDT. Thank you very much, Chairman Simmons, Ranking Member Lofgren and distinguished members of the subcommittee. It is truly an honor to appear before you today to discuss the topic of terrorism risk assessment.

I would like to cover three areas in this opening statement. I will briefly introduce you to the Center of Risk and Economic Analysis of Terrorism Events, called CREATE; I would like to provide some background on risk assessment and its uses over the last 30 years in various government agencies and private enterprises; and I would like to end by commenting on the uses, opportunities and important challenges of using risk assessment in the homeland security area.

CREATE was the first university-based center of excellence funded by the Department of Homeland Security. It was selected in 2003 in a competition of 72 universities and we started operations in March 2004. CREATE is located at the University of Southern California and has partners at NYU and at the University of Wisconsin and other universities across the country. Our main goal is to develop advanced risk assessment tools and economic tools for homeland security decisions.

Let me turn a little bit to risk assessment in the broader context. Risk assessment has a very long history, dating back to studies of nuclear power plant safety and spacecraft safety in the 1970s. Today, risk assessment is successfully applied in areas as diverse as medicine, business, environment, industrial safety and natural disasters. A typical risk assessment answers three questions: What can go wrong, how likely is it and what are the consequences? My overall impression is that risk assessment has been very successfully applied by identifying risks and by developing cost-effective solutions to reduce risks in these areas.

The application of risk assessment to terrorism is fairly new, providing new opportunities and challenges. Natural and engineered systems are "neutral" agents who don't seek out our vulnerability. Terrorists, in contrast, are the adversaries who attempt to attack us where we are weak, and furthermore they adjust their actions

in response to our defenses. This non-random nature of terrorism complicates risk assessment and requires the development of new tools.

In spite of these challenges, risk assessment has made considerable progress in the terrorism area in the past few years. An important distinction, as mentioned earlier, in risk assessment for terrorism is the difference between threat assessment, vulnerability assessment and consequence assessment.

I don't want to repeat what the previous speakers have said. I just want to bring one point clearly home, and that is that threat assessment is by far the hardest part of terrorism risk assessment. This deals with assessing terrorist motivations, capabilities and intent. Assessing vulnerabilities is somewhat easier, and we have developed tools based on project risk analysis to do this task.

Finally, the assessment of consequences, given a successful attack, as terrible as these consequences may be, can be pursued with relatively off-the-shelf methods that are usually provided by the national laboratories.

Another distinction is between the various levels of homeland security decision making. We typically distinguish between decisions on specific countermeasures; for example, specific decisions on MANPADS countermeasures.

The second area is prioritizing and resource allocation within a threat area; for example, prioritizing infrastructure threat targets, which is much of the topic of this committee.

Finally, the high level policy decisions having to do with resource allocation between broad threat areas; for example, within radnuke, biological and infrastructure threats.

Our recent studies suggest that specific countermeasure decisions can well be supported with risk assessments, and CREATE has made some contributions in this area which I would be happy to discuss with you later. We also see some progress in the use of risk assessment within threat areas. For example, in the past few years, several commercial risk analysis tools have been developed for a session risk infrastructure targets and prioritizing them.

Risk assessment at the highest policy level is difficult and will necessarily involve expert judgment and more qualitative forms of analysis. However, overall, I am very optimistic that risk assessment can improve our Nation's decisions to counter terrorism, and much progress has been made, but there are also many challenges ahead.

I thank you very much for this opportunity to address you.

[The statement of Mr. von Winterfeldt follows:]

PREPARED STATEMENT OF DETLOF VON WINTERFELDT

Chairman Simmons, Ranking Member Lofgren, distinguished members of the Subcommittee: It is an honor to appear before you today to discuss the topic of terrorism risk assessment.

I'd like to cover three areas in this opening statement. First, I will briefly introduce you to the Center for Risk and Economic Analysis of Terrorism Events (CREATE); second, I'd like to provide some background on risk assessment and its uses in the past 30 years in government agencies and private enterprises; third, I'd like to comment on the uses, opportunities and challenges of risk assessment in the homeland security area.

CREATE is the first university-based center of excellence funded by the Department of Homeland Security. It was selected in a competition of 72 universities and

started operations in March of 2004. CREATE is located at the University of Southern California with partners at the University of Wisconsin, New York University and faculty affiliated with the Massachusetts Institute of Technology. CREATE researchers are developing advanced risk assessment models and tools for homeland security decisions. We also study the economic impacts of terrorist events and develop computer models and analysis tools to assist decision makers in government and industry to allocate funds to counter terrorism.

Risk assessment has a long history—dating back to studies of nuclear power plant and spacecraft safety in the mid 70s. Today, risk assessment is successfully applied in areas as diverse as medicine, business, environment, industrial safety and natural disasters. A typical risk assessment answers three questions:

1. What can go wrong?
2. How likely is it?
3. What are the consequences?

In addition, risk assessments examine what can be done to reduce the likelihood of failures and the magnitude of consequences and to evaluate the effectiveness of alternative investments in improving safety. My overall impression is that risk assessments in these applied areas have been very successful by identifying risks and by developing cost-effective solutions to reduce risks.

The application of risk assessment to terrorism is relatively new providing new opportunities and challenges. Natural and engineered systems are "neutral" agents, who don't seek out our vulnerabilities. In these areas we also have a fair amount of experience and data that can be used to estimate probabilities and consequences. Terrorists, in contrast, are adversaries, who seek out our vulnerabilities and adjust their actions in response to our defenses. This non-random nature of terrorism complicates risk assessments and requires the development of new tools.

In spite of these challenges, risk assessment has made considerable progress in the terrorism area in the past few years. An important distinction in terrorism risk assessment is between threat, vulnerabilities, and consequence. When considering threats, we need to consider the motivation, capabilities, and intent of terrorist groups. This is probably the hardest part of terrorism risk assessment and there are no off-the shelf solutions for this task. CREATE researchers are working together with another university center of excellence—the Center for the Study of Terrorism and Response to Terrorism (START) at the University of Maryland—to develop risk analysis models for this purpose. Assessing vulnerabilities is somewhat easier. The key is to consider a wide range of threats and to assess the probability that an attempted terrorist attack is successful. CREATE researchers are using project risk analysis methods for this purpose. Finally, the assessment of consequences, given a successful attack, is quite straightforward and we can use off-the-shelf methods, for example, for modeling the dispersions of materials, spreading of infectious diseases, and so forth.

Another distinction is between the various levels of homeland security decision making. Recent studies by our CREATE researchers suggest that specific countermeasure decisions, for example regarding MANPADS countermeasures, can be supported quite well with risk assessments. At the next level are decisions on how to allocate funds within a specific threat area or across potential targets. We see some progress in this area as well. For example, in the past few years several commercial risk analysis tools have been developed for assessing risks of infrastructure targets. At the highest decision making level are questions about how much money to spend on, for example, radiological and nuclear defenses vs. biological defenses vs. infrastructure protection. Risk assessment at this level is difficult and will necessarily involve expert judgments and more qualitative analysis.

Overall, I am very optimistic that risk assessment can improve our Nation's decisions to counter terrorism. In other areas it often has taken years from the initial uses of risk assessment to mature applications. I believe that we can do better in making risk assessments useful in the terrorism area, but we also need to be aware of the many challenges we face.

Mr. SIMMONS. I thank you very much for those comments.

Our fourth witness is Dr. Henry Willis, who is a policy researcher with the RAND Corporation, where his research applies decision, analytical tools and risk analysis to help decisionmakers choose among competing resource management strategies or policy actions and options. Examples of his recent research include assessing risk-based approaches to allocating homeland security preparedness resources, reviewing current and proposed counter-

measures for protecting U.S. maritime transportation infrastructure, and assessing personal protective equipment needs of emergency responders working in a post-structural collapse environment.

Dr. Willis, welcome. We look forward to hearing your testimony.

STATEMENT OF DR. HENRY WILLIS, POLICY RESEARCHER, THE RAND CORPORATION

Mr. WILLIS. Thank you, Chairman Simmons, Ranking Member Thompson, Ranking Member Lofgren and distinguished members. I would like to thank you for giving me the opportunity to speak with you today about terrorism risk assessment at the Department of Homeland Security.

Many of my comments are based directly on a recently released RAND report entitled Estimating Terrorism Risk. I will make hard copies of this report available to the committee, and would like to request that the report be made part of the official record.

Mr. SIMMONS. Without objection, so ordered.

The information is maintained in the committee file.

Mr. WILLIS. Over the last 4 years, Congress and the Department of Homeland Security have made tremendous progress in maturing homeland security policy. Shortly after September 11, 2001, decisions were dominated by the use of crude indicators, such as population, which approximated consequences of terrorist events. Subsequently, policy moved to vulnerability reduction. And, more recently, Secretary Michael Chertoff has called on DHS to adopt risk-based decision making. The next step in this process will be the focus on risk reduction and cost effectiveness, but the U.S. Government is currently in the early phases of this stage.

With this as background, there are five recommendations from our work that are pertinent to today's hearing. First, the U.S. Government should consistently define terrorism risk in terms of metrics, like expected annual consequences. Critical infrastructure risk assessment is too often focused on potential consequences, either ignoring or under emphasizing factors that determine threat and vulnerability. Expected annual consequences take threat vulnerability and potential consequences into consideration in a rational way. Defining terrorism risk in terms of all these factors facilitates the incorporation of risk reduction as the goal of Homeland Security programs.

Secondly, DHS should seek robust risk estimators that account for uncertainty about terrorism risk and variance in citizen values. Given the tremendous uncertainties surrounding terrorism risk assessment, it is prudent to plan for the range of plausible futures that may play out. Many different models exist, and experts disagree on terrorist capabilities and intentions. Risk assessment should reflect all critical models and expert judgments. The challenge is to support a single decision, while still being able to identify how risk is distributed differently across different outcomes, such as fatalities or property damage, and also explain how the decision would change if more emphasis were given to a single type of outcome or perspective on threats and vulnerabilities.

Third, DHS should use event-based models to assess terrorism risk. Measuring and tracking levels of terrorism risk is an impor-

tant component of homeland security policy. These data provide insights into how current programs are reducing risk and when and where new terrorist threats may be emerging. Only event-based models of terrorism risk provide insight into how changes in assumptions or actual levels of threat vulnerability and consequences affect risk levels.

Fourth, relying on event-based models does not mean relying entirely on a top-down process. It is important to differentiate strategic risk assessment from risk assessment to support design or performance assessment or that to support tactical decisions. Strategic assessments might guide the distribution of resources that are not reallocated frequently. Design and performance assessment might be used to optimize or tune a response to a particular threat or protect a specific asset. Think of assessment used to reinforce the design of a nuclear power plant. Tactical assessments might be in response to intelligence regarding specific threats or events that have already occurred.

Of course, all are needed. I recommend that a top-down approach is most practical for strategic risk assessment, and estimates need not be as detailed as design or tactical risk assessment. The goal is to distribute resources in roughly the right places and in correct proportion.

On the other hand, I recommend a bottom-up approach to support design or tactical decisions. Here, more detailed models and analysis can be used to authorize spending on specific projects and justify current programs.

Finally, the U.S. Government should invest resources to bridge the gap between risk assessment and resource allocation policies that are cost-effective. The first step in this process is implementing annual independent risk impact assessments to evaluate how risk reduction funds have succeeded in reducing risk. These assessments will provide a feedback mechanism that will ultimately help increase of risk.

The second step is a capabilities-based assessment of the Nation's homeland security programs to document the unique contributions provided by each and ensure balance between the layered defenses that have been put in place.

I would like to thank you for the opportunities to address the committee on this important subject, and I look forward to your questions.

[The statement of Mr. Willis follows:]

PREPARED STATEMENT OF HENRY WILLIS, PH.D. [1]

Good afternoon, Mr. Chairman and distinguished Members of this Committee. I would like to thank you for the opportunity to speak with you today about terrorism risk assessment at the Department of Homeland Security (DHS). Many of my comments are based directly on a recently released RAND Corporation report entitled, "Estimating Terrorism Risk," which has been made available to Members of the Committee. This report is part of RAND's program of self-initiated research that is funded through the independent research and development provisions of our Federally Funded Research and Development Centers. It is the latest release by the RAND Center for Terrorism Risk Management Policy, which was established in

2002 to study terrorism risk management, insurance, liability, and compensation. I would like to request that this report be made part of the official record.SPELL

Over the last four years, Congress and the Department of Homeland Security have made tremendous progress in maturing homeland security policy. Shortly after September 11, 2001, decisions were dominated by the use of crude indicators, such as population, which approximated consequences of terrorist events. Subsequently, policy moved to vulnerability reduction and more recently, Secretary Michael Chertoff has called on the DHS to adopt risk-based decisionmaking. The next step in this process will be to focus on the risk reduction and cost effectiveness, but the U.S. Government currently is in the early phases of this stage.

The recently released draft National Infrastructure Protection Plan (NIPP) reflects this progression by defining an aggressive and comprehensive approach to risk assessment across sectors that affect the U.S. economy. As compared to earlier drafts of this document, it reflects adoption of Secretary Chertoff's guidance to use risk-based decisionmaking and represents the state of the Department's thinking on critical infrastructure protection. Specifically, it tries to take a balanced approach to incorporate: risk assessment; information sharing, feedback, and training; organizing and partnership with private sector; resource allocation; and long-range sustainability of protection efforts. Finally, the draft NIPP describes a framework that follows the best practices of risk analysis that are outlined in, among other places, the National Research Council in its foundational reports *Risk Assessment in the Federal Government: Managing the Process (1983) and subsequently Science and Judgment in Risk Assessment* (1994). These best practices require that risk assessments be: a) analytic, b) deliberative, and c) practical. For homeland security policy, these statements have the following translation:

a) Analytic

An analytic process requires addressing all three of the factors that determine terrorism risk: 1) threat, 2) vulnerability, and 3) terrorism, and where feasible, to do so quantitatively. Risk assessments must be repeatable so all parties can replicate, analyze, and understand them. However, the uncertainty inherent in this problem, particularly in the terrorist threat, implies that unlike most of our successful experience with these tools in the past, some new thinking about all plausible threats, not just the most likely threat, will need to be taken into account.

b) Deliberative

A deliberative process is necessary because the notion of a cold, analytic risk assessment is a myth. Values and judgment are part and parcel to the process and require transparency and a comprehensive discussion of outcomes. This is the only way to credibly address tradeoffs between risks to people from risks to property and risks from a conventional bomb, nuclear attack, biological attack, or even hurricane or other natural disaster.

c) Practical

Finally, risk assessment must be practical, meaning that data collection and management requirements must not be untenable and estimates should not be overly reliant on a single perspective or tool. This last point is where concerns may arise with the draft NIPP. These concerns relate more to implementing what is outlined rather than concerns with the content of the plan itself. Implementation will need to address natural disasters as well as terrorist threat as the plan is used. Questions remain about the practicality of implementing risk analysis and information sharing given limitations in the real world as to funding, time, and staff available. These issues have not been ironed out.

With this as background, there are 5 recommendations from our work that are pertinent to today's hearing.

First, the U.S. Government should consistently define terrorism risk in terms of metrics like expected annual consequences. Critical infrastructure risk assessment is too often focused on potential consequences, either ignoring or under emphasizing factors that determine threat and vulnerability. Expected annual consequences take threat, vulnerability and potential consequences into consideration in a rational way. Defining terrorism risk in terms of all of these factors

---

[1] The opinions and conclusions expressed in this testimony are the author's alone and should not be interpreted as representing those of RAND or any of the sponsors of its research. This product is part of the RAND Corporation testimony series. RAND testimonies record testimony presented by RAND associates to federal, state, or local legislative committees; government-appointed commissions and panels; and private review and oversight bodies. The RAND Corporation is a nonprofit research organization providing objective analysis and effective solutions that address the challenges facing the public and private sectors around the world. RAND'S publications do not necessarily reflect the opinions of its research clients and sponsors.

facilitates the incorporation of risk reduction as the goal of homeland security programs.

Second, DHS should seek robust risk estimators that account for uncertainty about terrorism risk and variance in citizen values. Given the tremendous uncertainties surrounding terrorism risk assessment, it is prudent to plan for the range of plausible futures that may play out. Many different models exist and experts disagree on terrorists' capabilities and intentions. Risk assessment should reflect all credible models and expert judgments. The challenge is to support a single decision, while still being able to identify how risk is distributed differently across different outcomes, such as fatalities or property damage, and also explain how the decision would change if more emphasis were given to a single type of outcome or perspective on threats and vulnerabilities.

Third, DHS should use event-based models to assess terrorism risk. Measuring and tracking levels of terrorism risk is an important component of homeland security policy. These data provide insight into how current programs are reducing risk and when and where new terrorist threats may be emerging. Only event-based models of terrorism risk provide insight into how changes in assumptions or actual levels of threat, vulnerability, and consequences affect risk levels. There are many types of event-based models in existence. In our report, we relied on the Risk Management Systems (RMS) Terrorism Risk Model. This and other insurance industry models could also be used to support homeland security policy. The national laboratories have made progress on detailed models of critical infrastructures and their interdependencies. Colleagues in academia are applying economic input-output analysis to understand these same dependencies. Finally, the NIPP points to RAMCAP, or Risk Assessment Methodology for Critical Asset Protection, which is based on a foundation for risk analysis consistent for methods used in reliability analysis and also with the National Research Council framework.

Fourth, relying on event-based models does not mean relying entirely on a top down process. It is important to differentiate strategic risk assessment from risk assessment to support design or performance assessment or that to support tactical decisions. Strategic assessments might guide the distribution of resources that are not reallocated frequently. Design and performance assessment might be used to optimize or tune a response to a particular threat or protect a specific asset. Think of assessment used to reinforce the design of a nuclear power plant. Tactical assessments might be in response to intelligence regarding specific threats (actionable intelligence) or events that have already occurred.

Of course all are needed. I recommend that a top-down approach is most practical for strategic risk assessment; and estimates need not be as detailed as design or tactical risk assessment. The goal is to distribute resources in roughly the right place and correct proportion. On the other hand, I recommend a bottom-up approach to support design or tactical decisions. Here more detailed models and analysis can be used to authorize spending on specific projects and justify current programs.

Strategic risk assessment ultimately needs event-based models. Until event-based models are more widely used to assess terrorism risk, density-weighted population is preferred over population as a simple risk indicator. Density-weighted population is simply a regions population multiplied by its population density. Our report found this metric to be reasonably correlated with the distribution of terrorism risk across the United States, as estimated by event-based models like the RMS Terrorism Risk Model. In contrast, our results suggest that population offers a remarkably weak indicator of risk, not much superior to estimating risk shares at random.

Finally, the U.S. Government should invest resources to bridge the gap between terrorism risk assessment and resource allocation policies that are cost effective. As I intimated earlier, Congress and DHS are only in the position to estimate risks and distribute resources where the risks are believed to be the largest. Ultimately, the goal should be to distribute those resources where they most effectively reduce risk. The first step in this process is implementing annual, independent risk impact assessments to evaluate how risk reduction funds have succeeded in reducing risk. These assessments will provide a feedback mechanism that will ultimately help increase reduction of risk. Such assessments would benefit the DHS grant programs as well as border and maritime security programs like US-VISIT, C–TPAT, the MTSA, and TSA's baggage and passenger screening and profiling programs. The second step is a capabilities-based assessment of the nation's homeland security programs to document the unique contribution provided by each program and ensure appropriate balance to the layered defenses that have been put in place.

I would like to thank you again for the opportunity to address the committee on this important subject and I look forward to answering any questions you may have.

Mr. SIMMONS. Thank you all very much. I have a couple of questions that I would like to ask, and then we will go back and forth in accordance with our regular order.

My first questions are to Ms. Smislova. Critically important to the success of your mission and your organization is information sharing, information sharing with the Intelligence Community to make sure you are getting the terrorist risk assessments with regard to intents and capabilities, but also information sharing with those private sector entities that manage the infrastructure that we are trying to protect, whether it be nuclear power plants or bridges or chemical facilities.

It occurs to me that traditionally the Intelligence Community does not like to share information. I am sorry about that, but they like secrets. If you really like secrets, you don't tell anybody your secrets.

Secondly, private sector industries may not be willing to share information on vulnerabilities for fear that if there is an incident they may be held financially liable for the consequences.

So, how are you doing with these twin sets of challenges to information sharing? What is your status report as of this moment?

Ms. SMISLOVA. Yes, sir. We in the Intelligence Community like to just share, as you know, with each other, and we are accomplishing that through the Office of Intelligence and Analysis. We believe that through HITRAC, actually putting the infrastructure protection specialists together with those Intelligence Community professionals, is the best way to enhance that relationship and that communication.

Our infrastructure protection specialists through the other offices in the Office of IP communicate daily with the infrastructure sectors. They are the ones who have developed the relationships and the contacts with the infrastructures and what their situation is on the ground and their daily information about what is happening in their sector. So every day when we are working on common goals and common work projects, the intelligence analyst is working with the infrastructure protection person. So we actually are receiving that information that is not traditionally looked at by intelligence.

Mr. SIMMONS. And with regard to that interaction or that activity, what sort of products are you producing and how are they disseminated?

Ms. SMISLOVA. Yes, sir. We are actually producing a basic foundation document for every critical infrastructure or key resource that obviously is expanded beyond the critical infrastructure of transportation and would include one on aviation, maritime, railroads, mass transit and highways. So there are about 24 different products that we are producing.

We are doing these in conjunction with our actual infrastructure operators and owners, and I think that is what does make us quite unique. While we have the benefit of actually all the information that our Intelligence Community colleagues have about the enemy, we are actually looking at everything that is available for the U.S. Government in all different classified areas of what the adversary wants to accomplish and how.

We also at the same time have a dialogue, because we are this hybrid of intel professionals and non-intel professionals, we have a

dialogue with the actual infrastructures. So through the framework of the NIB, we have committed to producing these foundation documents on what the terrorist threat to that particular structure or infrastructure might be.

Mr. SIMMONS. Thank you.

Dr. Winterfeldt, you made an interesting comment. The non-random nature of terrorism complicates risk assessment and requires the development of new tools. For a number of years I served as a military intelligence officer in Vietnam, and we would collect information and make predictions about enemy attacks. The military units in responding to those predictions would take defensive measures, which would be observed by the other side and when they would see the defensive measures being taken they would realize it was a tip-off so they wouldn't conduct the attack. Then our own side would say you guys are wrong again.

It occurs to me in a free and open society, such as ours, where we discuss our vulnerabilities and our efforts to protect our infrastructure, that the opposition is fully aware of those efforts and can adjust for that.

How do we account for that in our risk assessment?

Mr. VON WINTERFELDT. Thank you very much. That was a very interesting question, and something that we are grappling with in many ways.

We actually have some of our team members who are looking at this from a red team and blue team perspective. They are looking at it from a game theoretic perspective. Actually, I see the greatest hope in sequential games, very much playing out in a modeling form the situation you described, which can even lead you in some cases to protect information about defensive measures, or, potentially, I hate to say this, provide misleading information about protective measures.

I will just give you one example. Should we always say that we are doing 10 percent or 5 percent inspections of our cargo? Well, maybe we can do 10 percent and then claim we use 50 percent. You remember the case of the cameras at the intersections, half of which never worked. So there are a lot of interesting issues.

We certainly have no silver bullet nor simple answer to that. But that is exactly the kind of topics we are studying as we are working at CREATE.

Mr. SIMMONS. Thank you. I see my time has run out. Ms. Lofgren.

Ms. LOFGREN. Thank you. I am glad to have Ms. Smislova here, because I have a continuing interest, as I mentioned in my opening statement, in the National Asset Database. I will just express some frustration. I am not alone in this frustration. But this has now gone on for a couple of years, and we have had several classified discussions, and I remember the first time it was a bipartisan group and informal, and I asked to see the database for my county because I know it well and the members from other parts of the country did the same, and all of us were struck by how preposterous the list was. I recently received an updated list, and it was still preposterous.

So my question is, when do you think this National Asset Database will be complete, at least in its—I realize it will be updated,

but delivered? When do you think that delivery will be to the Congress?

Ms. SMISLOVA. I am sorry, ma'am. I actually don't know the answer to that particular question. What I do know is that the National Asset Database is intended to catalogue all of the assets in this enormous country of ours. I know from notes I took during your opening statement that your goal here is to conclude what to protect first and why, and that is actually the issue that we are trying to start with in HITRAC.

From my perspective as the senior intelligence person assigned to HITRAC, that is the focus of what we have put our efforts towards, trying to get a better understanding of this particular enemy, this adversary who we know wants to attack us here in the United States, what does he want to attack and how?

By using information that is available through the National Asset Database, we have been able to crosswalk and narrow some things down. So we try to determine what does the adversary want to accomplish, what are his goals, and then how can he accomplish this. And because we don't have specific data that he wants to hit this building or another building or a specific mass transit fleet or anything that granular, we try to crosswalk it and say these are the things we think we need to protect first and why.

But I will bring your other question back for the record, ma'am.

Ms. LOFGREN. I appreciate that. Along with that, and if you don't know today, that is fine, but if you can get back I would appreciate it. Part of the problem I discovered was—I met not only with DHS staff, but also with—we all go home every week—with people in local government, with the State officials, trying to find out what was happening from their point of view, and learned in doing so that there had been an asset limit on how many assets could be reported, which is a preposterous way to proceed because in Santa Clara County, for example, it is a county of just shy of 2 million people. It is Silicone Valley. There are many, many assets. To be limited to 18 in Santa Clara and 18 in Shasta County, where you might be hard pressed to come up with 18, is ridiculous. So I am hoping I can get information on whether that that policy has been changed as we urged that it be.

Let me ask a question for Dr. von Winterfeldt. We are being asked, and we agree, that Homeland Security dollars should be spent in a strategic way to protect our assets best, and I think all of us agreed with the Secretary that it automatically ought to be risk-based, it shouldn't be some formula like an entitlement program, that is not the way to do. But it seems to me central to that effort is the development of this National Asset Database and the database is not complete, it doesn't prioritize critical infrastructure assets across the 17 sectors identified in HSPD–7.

In your view, how significant an obstacle is the failure to complete this database to meaningful terrorism risk assessment at the Department?

Mr. VON WINTERFELDT. Well, I believe that it will be very useful to have that database as a start. Let me also say where I see this heading down the road, and that is to do a good job on critical infrastructures with the database, or even with part of the database, is you have to work yourself from the specific infrastructure assets

up and roll it up. You can't do a risk analysis on the high level, not even at the county level, not even at the State level, unless you know what is going on with the particular assets and what you can do with it.

So CREATE, for example, is now engaging with the California Department of Homeland Security to look from the bottom-up at the assets and the infrastructures that California has identified as important and start to build a risk analysis at that level and going up. Of course, the ultimately comparison between the States or even the urban initiatives in the urban areas can only be done if you have a complete set of assets and infrastructure elements.

Ms. LOFGREN. My time has expired, so I will save my further questions for the second round.

Mr. SIMMONS. The gentleman from California, Mr. Lungren.

Mr. LUNGREN. Thank you very much, and I understand what Ms. Lofgren says when she compares her county to Shasta County, but I do hope that Shasta Dam is on that list of critical infrastructures and so is the headwaters of the Sacramento River, which provides about one-third of the water for our whole state.

Ms. LOFGREN. I love Shasta County. Let me clarify that. I think Shasta County is a wonderful place.

Mr. LUNGREN. I keep calling it HITRAC, but you want to call it HITRAC. See, when you are an English major, you divide things into proper syllables, and HITRAC sounds better than HITRAC.

As I understand, HITRAC or HITRAC is a point of contact for summary and trend analysis for suspicious activity reporting, which I guess we call SARS, even though that has other indications these days, and they are supposed to be sent in by public and private individuals at local levels to provide warning signs of potential terrorist attack.

How effective is this program? How much is it really on? To put it another way, if I happen to be a manager of an asset in northern California, private or public, how well am I informed of these suspicious activity reports? How do you see that reflected in what you receive in your shop?

Ms. SMISLOVA. The suspicious activity reports typically are coming from industry through the Information Sharing Advisory Councils, the ISACs, or directly to our operations center. Sometimes we get suspicious activity reporting just from American citizens. They will call them in and they are called Patriot reports.

Mr. LUNGREN. My question is, how do I know that? How do people know that?

Ms. SMISLOVA. We distribute, disseminate, our products back again through that same vehicle, through the ISACs, through the Homeland Security advisers. We do send our reports to the JTTFs. That is all distributed.

Mr. LUNGREN. I guess my question is, how comfortable are you in the belief that there is a high level of understanding of your activity and the need to report these things?

Ms. SMISLOVA. It is spotty, sir. Some industries we have been able to dialogue with and we have been able to discuss with them what we are trying to accomplish with the suspicious activity reporting, and some industries or entities we have not. It is easier at this point to have outreached to ones that are more organized.

So for example, the electrical power grid, we have a dialogue with the people that run that particular infrastructure.

It is more difficult with the shopping malls of America. We are trying to tailor our products to make sense to those that are protecting the different critical infrastructure, but we do realize that each group that runs the infrastructure is diverse, and that is again where I would get back to the requirement for the Department to outreach and dialogue with the individuals.

Mr. LUNGREN. Let me ask you this question: This weekend there are literally going to be millions of people attending football games at major colleges, universities and in the NFL. Can you tell me from what you know, are people who run those operations cooperating with the Department of Homeland Security such that you are getting reports of any suspicious activity of this nature?

Ms. SMISLOVA. We actually do deal with the commercial services sector. I also sent a HITRAC employee to brief the security people that do the college football, all the college football security thing, have been briefed by us on what to look for or what we believe would be suspicious activity that might indicate an attack was pending.

Mr. LUNGREN. You have told them that you have got this. Do you get reports from them?

Ms. SMISLOVA. We get reports from the commercial services sector, yes.

Mr. LUNGREN. I guess I still have a little bit of time. For the whole panel, this seems to be a crucial part of protecting critical infrastructure, making owners and operators aware of what to look for in terms of suspicious activity. For the other panelists, what is your sense of the awareness of this program and do you have any recommendations on what we would do to make it more effective?

Ms. WORMUTH. I certainly can't speak to the public or industry's awareness of HITRAC in particular.

Mr. LUNGREN. That is not what I am talking about. I appreciate listening to all of what you have to say, and it sounds good in theory. But if it breaks down, if all we are doing is talking about it and no one knows what information needs to get to us for this—I am just trying to find out if any of you have a sense of how broadly understood this is, how much is this actually working? Are we sitting here talking theoretically about what would sound like a great idea, but you can't analyze anything unless you get data to analyze?

Ms. WORMUTH. Congressman, I would say I am aware of at least New York City, and I would suspect some other major cities, have programs that are focused on going out and talking to businesses, industry owners, and again it sounds like very similar to what Ms. Smislova was speaking to, which is talking to those folks in the private sector about what to look for and what type of activity to report. I believe the program in New York City is called Hercules. My memory may be wrong, but some major cities certainly have programs designed to try to make the private sector aware and alert them to either report in to city governments or the State Homeland Security managers.

Mr. VON WINTERFELDT. At CREATE we work a lot with local government officials, and I know there are many mechanisms for them

to report at the local level. I don't know how the reporting works from there to the Department of Homeland Security or back, so I can't comment on that. But I do believe that the local level works well.

Just recently in L.A. there was a discovery of two events, a discovery of two suspicious females that were taking pictures. They were pursued and eventually apprehended, and it turned out to be a false alarm. So some things seem to be working at the local level. I am not sure how the national and local level are communicating.

Mr. LUNGREN. Thank you.

Mr. SIMMONS. The gentleman from Pennsylvania, Mr. Dent.

Mr. DENT. Thank you, Mr. Chairman. Ms. Smislova, I get a lot of comments from my folks back home in Pennsylvania, from the Homeland Security folks and others at the local level, and my main question to you is this: Are any local Homeland Security agencies detailed to HITRAC, or HITRAC, whatever the case may be?

Ms. SMISLOVA. Not at this time, no, sir.

Mr. DENT. Regarding your evaluation of risk, what sort of input do you get from State Homeland Security or local first responders, I guess you don't get any, in making these evaluations? Do you get any input from them?

Ms. SMISLOVA. Yes, sir, we are. We are trying to outreach to different customer sets as we are developing them, and we also are briefing some States and first responders and then incorporating their comments or their suggestions.

Mr. DENT. So I guess the broader question is what do you see as the role of these local groups in helping determine threat vulnerability and consequences?

Ms. SMISLOVA. We see the role as large and expanding. We have connectivity with every State and we talk to every State. We hope that would be our goal, to expand our production efforts to deal with at least all the major metropolitan areas.

Mr. DENT. I guess my question is, my main comment is, these folks at the State and local level really want to be I think a greater part of this process. Sometimes I feel as if the information they receive is not helpful, that they just don't have the ability to process what gets sent down to them from Washington. This information sharing, something gets lost between the Federal and State and local levels, and they really want to be involved more than they have been.

I guess the question would be, how do you go about disseminating risk evaluations to local communities that may in fact be vulnerable to attack, and how do you ensure that risk assessments are timely, relevant and helpful to local communities that must ultimately be forced to respond to any such attacks? They worry about the timeliness and relevance of the information they receive. How do you address that?

Ms. SMISLOVA. Again, our goal is to interact more often with the State and the local governments. We do have people from the State and local entities deployed in our operations center. We deal with them on a regular basis. We travel out to States and local places. I have two people today in Chicago discussing some risk assessments and plans for additional products. So that is just how we have begun with our work.

Mr. DENT. I have raised these same questions to the folks from the ASSOC and elsewhere, and anybody else feel free to chime in if you have any points on this issue. I would be glad to hear it.

Mr. WILLIS. I would like to say that I agree with the assertions that have been made that local intelligence is a very important part of understanding threat. I think it also points to one of the observations we found in our report, that risk assessment can't be done only from the top-down, but also sometimes from the bottom-up.

My colleague, Dr. Winterfeldt, talked about work they are doing in California that is very much bottom-up where a lot of the information is. So there is a need to look at doing these risk assessments from both directions.

Mr. DENT. No further questions. I yield back.

Mr. SIMMONS. I thank the gentleman. We are going to go a second round, if that is all right.

Let me pick up where my colleague left off on the issue of top-down versus bottom-up. First of all, Dr. Willis, you said in your statement that tremendous progress has been made in maturing Homeland Security policy, and I would agree with that, even though I certainly understand my colleagues' frustration when miniature golf appears on a list somewhere. But I would hope that is an anomaly and not characteristic. I think progress has been made.

I think it is an impossible task to secure everything from everybody. If you try to do that, you will certainly fail. So you have to prioritize.

I think information sharing is very difficult to do, but I think people at a local level are somewhat aware, in some cases more than somewhat aware, of what we are attempting to accomplish.

So the challenge to me really is have we put in place a system that is sophisticated enough that not only does information come down from the top, presumably sensitive information or analytical products that the local community does not have the capacity to produce, but does the system allow local information and observation to go back up? Do we have a dynamic or a virtual system, in other words? And do the local folks have the tools and the networks to interact with the State and the Federal folks? Are we there yet or are we not?

Mr. WILLIS. That is a very good question. I will try to comment first broadly on where I think these tools and approaching networks are for risk analysis, and then also in terms of threat and passing threat information. I have not studied that as much but will check back with my colleagues at RAND.

In terms of risk analysis, what I have seen in all the States is organizations to try to link regionally to the State and make connections. In terms of tools, recently the Department of Homeland Security has released the draft National Infrastructure Protection Plan. In my written testimony I have included a few comments about that. I will try to summarize a few of the key points because I think it highlights some of the important points about the tools that are starting to be provided.

I would like to say, acknowledge, that RAND Corporation has been providing support to the Department of Homeland Security in

developing that plan. I myself have not personally been involved in that but have been asked to comment on it.

The key points I make about the NIPP is that it is comprehensive and it addresses all sectors. It is realistic in that it points out that you can't treat these sectors with a cookie cutter approach. Water is different than telecommunications, et cetera.

Where there might be—it is also laying out a common framework for doing risk analysis. This will help provide some structure to the local people who would be doing the analysis and also aid in comparison across assessments that come. Where there might be concerns is on implementation, because this is a very complex and resource-intensive approach, and that is where I would go back to my comments that we need to look for ways to trim the tree, we can't wait until we get all the assessments in to respond, and a combination of a bottom-up and top-down approach is necessary.

Mr. SIMMONS. In the brief time I have remaining for Ms. Wormuth, you made comments about National Intelligence Estimates and you made comments about a National Risk Assessment. The National Intelligence Estimate on Iraq's WMD of October 2002 was wrong, inadequate information, in my opinion, analysis based on inadequate information. So now we shift quickly to National Risk Assessment. Again, we don't know what we don't know.

Is this an exercise that is going to save the country, or is this an exercise that we engage in because we sort of know how to do it so we are going to do it?

Ms. WORMUTH. Thank you, Mr. Chairman. I knew when I made a comparison to a National Intelligence Estimate that I was opening myself up into a risky area, because not only can NIEs be wrong, they are also often viewed as relatively watered down and sort of lowest common denominator products.

That said, in my opinion, I think the only alternative to trying to come up with some sort of strategic level homeland security risk assessment is to not use a risk-based approach at all, which to me seems more perilous than trying to go through a structured risk assessment process and perhaps getting it only 80 percent right.

So I would argue that yes, there are dangers, but I think that there is not a better alternative. I think two broad advantages to risk assessments are that they will force policymakers to go through the myriad sets of threats and vulnerabilities in a structured way, and it really allows you to unpack some very difficult problems, as opposed to what I think many have observed is a tendency sometimes to try and allocate our resources to essentially the last war or sort of the new sexy thing.

Lots of money went towards aviation security because 9/11 was essentially an aviation-based event. Biological threats are very much in the news and a lot of resources are spent there, although for very good reasons.

One other thing I would emphasize is that I think while certainly factoring in very specific intelligence and looking at motivations and looking at intentions is very important, I also think there is a lot of wisdom to taking perhaps what I would call more of a capabilities-based approach, again, perhaps coming out of my DOD background. But to a certain extent, I think there is some utility at looking at threats from the perspective of simply what is avail-

able in terms of different weapons systems, in terms of different delivery systems, to somewhat more generic terrorist groups that are fairly well resourced, and at least thinking very broadly, because—I think because it is so difficult once you start getting into intentions.

Many, many people weren't even particularly aware of al-Qa'ida before 9/11. So I think there are definitely challenges in trying to do a strategic level assessment, but to me it is very much still—the benefits far outweigh the risks.

Mr. SIMMONS. Thank you for that answer.

Ms. LOFGREN.

Ms. LOFGREN. I want to get back to the National Asset Database, because I am hoping we can make some progress on it. Before I do, I just want to say I actually did check with people in the know and found out that there was no reason why the miniature golf course was on the list and that the people of San Jose should not worry about playing miniature golf. It could be dangerous in terms of the balls hitting people, but there is no other apparent threat.

In looking at how this has been put together, I think the chairman is right, we need to look at the systems in place to see whether they are going to yield information that is valuable. One of the things that became apparent to me was that we had passed really local police departments to come up with the list of critical infrastructure, and they are doing a terrific job, their very best. This is not critical of their efforts, but there are certain things that they are just not in a position to know; for example, telecommunications physical infrastructure or certain cybersecurity issues. It is just not within the purview of the police department for the most part.

There were some things actually that the fire department might know that the police department would not know, and they were not included, and the health people were not included, and the private sector people were not included.

So I am wondering if there has been a change in the structure of who is included so that we can make sure that the critical infrastructure, all of it, is actually in this database.

Does anyone know the answer to that?

Ms. SMISLOVA. Ma'am, we would be happy to come back and give you and your staff a briefing on the NADB. We can arrange that for you.

Ms. LOFGREN. But you don't know the answer to that?

Ms. SMISLOVA. No, ma'am, I do not.

Ms. LOFGREN. Maybe Dr. Winterfeldt would know this. At one point the Department asked the—I believe it was the sheriff's department, it might have been the police department, in the City of Los Angeles to lead a pilot project, to change how the database, the National Asset Database is put together. Are you familiar with that?

Mr. VON WINTERFELDT. No, I am not specifically familiar with that.

Ms. LOFGREN. I would like to know—

Ms. SMISLOVA. Is that Project Archangel or Constellation?

Ms. LOFGREN. Archangel.

Ms. SMISLOVA. Yes, ma'am, I was actually briefed on that today by the Los Angeles Police Department, who was visiting. It is not

a National Asset Database, but it is a way to map the infrastructure of Los Angeles, and that actually is being done by the police department in conjunction with the Department of Homeland Security.

Again, it is not a system to prioritize, but rather to actually come up with a map so that when information is received, intelligence information, and it says something specific, that you are able to more quickly and rapidly come up with a facility list.

Ms. LOFGREN. That is different than the briefing I got. So perhaps it is more. But it seems to me that there needs to be some strategy. When I saw the list, there is shopping centers and there is a check cashing office in L.A. and stuff like that. I thought why would this stuff be there?

I can see if you received a threat that had something to do with shopping centers, you would want to know where all the shopping centers are. That is a good thing to know. But since our risk assessment really relates to our vulnerabilities and the consequences of activities, if you don't have a different list for—if you want to take down the water supply of southern California, there is three or four different ways you can do it, none of which are on the list.

So it seems to me that there needs to be—and I haven't seen it yet in the Department—any kind of a strategy for what would have a cascading both economic and also physical harm consequence that is connected with infrastructure so that as threats come in, we can lay those threats across what is a critical—

Ms. SMISLOVA. Right. We do, ma'am, work with the sector specific agencies to identify their top priority places. We have several of those sectors actually completed. That is a different effort, ma'am, yes. We can come back

Ms. LOFGREN. It is very mysterious, because we were told one thing about this database in the Congress and now apparently it has morphed into something else. So long as the job is getting done, I assume that is fine, but we have to really become convinced that the job has been done, and it is a long time since 9/11. We have wasted a lot of time, and I have some real concerns that we are not yet really ready and where we should be. So I will look forward to getting a further briefing on this.

I see that the red light is on, and I yield back, Mr. Chairman.

Mr. SIMMONS. The gentleman from California, Mr. Lungren.

Mr. LUNGREN. Thank you very much, Mr. Chairman. In your testimony, I notice you talk about the formal challenges involved in risk assessment in the area of terrorism, but you say despite these formal challenges, it is absolutely worth the time and effort to develop robust homeland security risk assessments that can guide our planning and policy development.

Then, Dr. Winterfeldt, you talk about how successful risk assessments have been in medicine, the business environment, industrial safety, natural disasters, how it is relatively new in the area of terrorism, but in spite of these challenges, risk assessments have made considerable progress in the terrorism area in the past few years. I would therefore say you indicate it is a tool that is automatically to be utilized at the present time.

Here is my question: It is easy for us once we have determined what the risks are and what the most vulnerable targets are, if

they are publicly owned, for us to command certain things to be done or for us to put as much money, government money as we can to it. But within the universe of critical infrastructure, a lot of stuff is owned by the private sector.

A couple of years ago, Congress felt it necessary to pass TRIA, a back-up to the regular insurance program. We are considering now to reauthorize it. I happen to be one of the people who thinks it is necessary given the still existing uncertainties in a terrorist scenario for the private sector. But one of our obligations here is to utilize something like try to see what the insurance industry, how the insurance industry plays in all of this, so that perhaps instead of us regulating something or mandating certain best practices or providing government incentives by way of tax policy, the private sector makes some adjustments in terms of what insurance companies are supposed to do, risk assessment.

How satisfied are you that the kind of information we have talked about that goes to DHS and is supposed to help drive policy, that that information is available such that private sector owners and the insurance industry can make the kind of judgments that will drive us towards the best business practices for a security purpose in light of what the true risks are out there?

Mr. VON WINTERFELDT. Perhaps I could give it a start. Actually CREATE put together a conference just a few weeks ago on the reissuing of TRIA and we are fairly familiar with these issues, together with RAND by the way.

It is a real difficult question of how you transfer the risk issues from the public back to the private sector. There ought to be self-interest in the private sector to protect themselves against terrorist events and I do not see it happening right now. This may be lack of information, it may be that they do not have the money or the capital to do it so they are looking to terrorism insurance. I am not sure that is a right solution either. The insurance only covers the asset when an event occurs. It does not do much in terms of protecting the asset against terrorist attacks, although properly implemented with insurance breaks and things like that it ought to do that.

Mr. LUNGREN. You have fluctuating premiums depending on what you are doing with respect to security. At the same time I could construct an idea of a hotel, for instance, which we know are targets of terrorists, American-identified hotels. And the more that we protect public sector assets it seems to me if I am an terrorist, I look at the softer targets of the private sector. We could drive the hotel industry in such a direction that they basically make all of their hotels look like fortresses and moats and destroy the industry because no one wants to go to a moat—a fortress for a vacation.

And what I was trying to figure out is how we establish a balance. And if we do not have the information available, it is even more difficult for us to get to the point as to where we want to go. And so my question really goes to the issue of are we in your judgment—have you seen, are we in the government when we gather this information, are we doing a good enough job of getting that out to the private sector, including the insurance industry, such that they can start to make rational judgments as to where they want

to go and have some guideposts and where we can sort of push people to best business practices?

Mr. VON WINTERFELDT. Very quickly and then I will pass it on to my colleague to my right. The insurance industry increasingly is turning to private companies to do these risk assessments for them. There are several companies, one is the one that Dr. Willis worked with, that do the risk assessments before the assets. So I do not see it necessarily happening only through information exchange between the Department and the private assets, but they are particularly interested in finding out which assets are threatened and make decisions about risk and premiums and insurance and things like that.

Let me stop right here and ask Ms. Wormuth.

Ms. WORMUTH. Congressman, certainly the fine points of the issues related to the insurance industry are well outside of my expertise. I would say one thing. I do think that—two things, I think Dr. Winterfeldt noted that there should be some self-interest on the part of industry to themselves take on some of the preventive measures. Because, of course, if they are attacked and their operations are essentially grounded for a period of time, that is not in their own interests.

But I think part of the challenge, we would be helped I think in convincing our colleagues in industry of the types of steps they need to be taking. If we could again walk them through in a logical, structured way, here is how we have come to this assessment and this is why—and I am just posing this as a hypothetical, which is why, chemical industry, we believe that you all do pose a high risk versus another particular industry which may be a lesser risk and we would like you all to consider these types of measures.

I think we would be able to better make that case to partners in industry if again we had a structured, defensible strategic assessment that we could walk them through in broad terms to help them see how they compared to other folks in industry.

Mr. LUNGREN. One of the concerns I have is how do we make sure that the information flows in both directions? How do we encourage industry and other people to get information to DHS and how do we encourage DHS and government entities to share enough of the analysis and information that people understand in an intelligent way what the risks are so that it will be in their self-interest to do that?

Because as the chairman has suggested, we have a culture in government which is not to share information. Give me the information and I can trust myself, but you are not going to get any of that out there. And I think it is a continuing problem because of the nature of the different functions we have. But in this area, if all we do on the government side is believe that government action is the sole universe in which we can deal with the threat, we are going to short ourselves from so much more activity that could be done of self-help and ultimately protecting us collectively, and I am just trying to raise these issues and look for as much information as I can.

Ms. WORMUTH. Sir, I take your point completely and I am sure Ms. Smislova can speak to it in more detail than I can. But in my experience working with organizations that work with DHS, I have

actually been pleasantly surprised in many instances at how much DHS is doing to try to reach out to industry and my outside observation is that there has been a lot of emphasis on that. They are working with folks through the HITRACs. I know that other elements of DHS are trying to work with State and local and private sector organizations and I think certainly that framework is not fully in place but my experience has been that DHS is very much trying to seek input from the private sector and from the public.

Mr. LUNGREN. Thank you.

Mr. SIMMONS. Please.

Mr. WILLIS. May I add one point on that?

Mr. SIMMONS. Please.

Mr. WILLIS. I agree with Representative Lungren that these are very important questions you are raising and since this panel is about risk analysis, I would say that I think risk analysis can answer many of these questions. In fact, RAND, through the Center for Terrorism Risk Management Policy, has been working with Risk Management Solutions as one of the insurance modeling groups that does some of this, and we would be happy to share with you some of the work that we have been doing to try to share that information. The information sharing actually goes both ways. I have been working with Risk Management Solutions and the Department of Homeland Security HITRAC to see how the type of modeling used in the private sector can inform DHS's risk assessment. Thank you.

Mr. SIMMONS. Do any members of the panel have any additional questions they would like to ask?

Any additional comments that the panel of witnesses would like to offer for the good of the order. Doctor? Anybody?

Mr. VON WINTERFELDT. I just wanted to make one comment. It is very important, and you raise very important issues. In many agencies that started risk assessment, starting with the Nuclear Regulatory Commission in the 1970s, this is when it was new stuff. It took years for risk assessment to mature to, filter through all parts of the agencies and to become a truly useful tool. So maybe we are hoping for too much. Maybe we are expecting for things to come too quickly. We are pushing. But I am certainly hopeful that risk assessment will be useful and used down the road in the Department more and more effectively.

Mr. SIMMONS. Anybody else have a final comment they would like to make?

Ms. SMISLOVA. Only to point out that Secretary Chertoff has appointed a new Assistant Secretary for the Private Sector as one of his developments under the reorganization and hopefully that will assist us in enhancing our outreach as a department to the private sector.

Mr. SIMMONS. Thank you all very much. I appreciate your coming here and your testimony. If members of the committee have additional questions for the witnesses, we will ask you to respond to those in writing and the hearing record will be held open for 10 days.

I would also like to conclude with an observation. On the week of September 11th I traveled to New York on a Friday with the President, and I represent the State of Connecticut. We lost people

on 9/11. My daughter actually was living in New York at the time and never returned back to her apartment because of the damage of 9/11.

As I stood there and looked at the devastation I was overwhelmed by the immense scope of it. Standing and looking at the burning remains of the World Trade Center, even as a Vietnam veteran, I would say it was probably one of the most devastating things I ever experienced. And then as we went back to the airport, took off and flew back to Washington we circled once and came over the top of the New York City and from that perspective the World Trade Center was simply a very small spot with a very small wisp of smoke coming up from it and the great expanse of New York, New Jersey and Long Island as well as Westchester County and Fairfield County, Connecticut seemed like an immense piece of property or real estate.

I guess what came across in that was how truly huge our country really is. What an extraordinary set of infrastructure we have and how difficult it is to refine our risk assessment to the point where we can cover it successfully. It is not easy. And I think, Doctor, you put your finger on it. This is going to take time. Now we as Americans are impatient people. We like our food in 15 minutes or less. We like everything to be very quick. But working on this problem is not easy to do.

So we thank you for the expertise that you bring to the table and wish you all the best as we pursue this issue into the future.

Without objection, the subcommittee stands adjourned.

[Whereupon, at 4:30 p.m., the subcommittee was adjourned.]