BUILDING A PARTNERSHIP STRATEGY: IMPROVING INFORMATION SHARING WITH STATE AND LOCAL LAW ENFORCEMENT AND THE PRIVATE SECTOR

HEARING

BEFORE THE

SUBCOMMITTEE ON INTELLIGENCE, INFORMATION SHARING, AND TERRORISM RISK ASSESSMENT

OF THE

COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES

ONE HUNDRED TENTH CONGRESS

FIRST SESSION

MAY 25, 2007

Serial No. 110–42

Printed for the use of the Committee on Homeland Security

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

U.S. GOVERNMENT PRINTING OFFICE

48–917 PDF WASHINGTON : 2009

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

COMMITTEE ON HOMELAND SECURITY

BENNIE G. THOMPSON, Mississippi, *Chairman*

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

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

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

SUBCOMMITTEE ON INTELLIGENCE, INFORMATION SHARING, AND TERRORISM RISK ASSESSMENT

JANE HARMAN, California, *Chair*

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

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

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

CONTENTS

BUILDING A PARTNERSHIP STRATEGY: IMPROVING INFORMATION SHARING WITH STATE AND LOCAL LAW ENFORCEMENT AND THE PRIVATE SECTOR

Friday, May 25, 2007

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

The subcommittee met, pursuant to call, at 1:06 p.m., at Bellevue City Council Chambers, 450 110th Avenue NE, Bellevue, Washington, Hon. Jane Harman presiding.

Members present: Representatives Harman, Dicks and Reichert.

Ms. HARMAN. The subcommittee will come to order.

The subcommittee is meeting today to receive testimony on improving information sharing with state and local—law enforcement and the private sector, and before we begin I would like to yield to our ranking member, Dave Reichert, for a matter of personal business.

Mr. REICHERT. Thank you, Madam Chair.

I just want to take a moment. I think we would, all of us here, as community members, be remiss if we didn't just take a moment to recognize the passing of our good friend Norm Maleng, so if we could just—I'm not going to make a long speech. We all know how much he meant to each and every one of us in this room, how much he meant to all of us in this community, but if we could just take a moment, Madam Chair, a moment of silence in honor of Norm's service and also maybe a personal and private prayer for their family and for their peace and strength.

Thank you.

[Moment of silence.]

Mr. REICHERT. Thank you, Madam Chair.

Ms. HARMAN. Thank you.

Thank you both for inviting me to this beautiful city and this beautiful location on a sunny day.

I have been to Seattle many times, never in sunshine, so I think having this hearing is a good omen.

Less than a week ago, 11 time zones away, I was in Baghdad and Ramadi, Iraq. It's a tough place to visit. I'm sure some of you have been there.

One thing I came away with is that al-Qa'ida is very real in Iraq, but I also know from other travels that al-Qa'ida is real and growing around the world.

This is just one of the major threats that could come our way.

I also know that about 150 miles from here at the Canadian border in 2000 a man named Ahmed Rasam was apprehended due to the good work of a customs agent.

Ahmed Rasam was driving a car with a trunk full of fertilizer, and the bomb, that he was going to put together, was intended to blow up at Los Angeles International Airport.

That gets my attention since my congressional district surrounds Los Angeles International Airport, and LAX is the airport target in America that has been identified several times by al-Qa'ida as a place that it would like to hit.

So it brings home to us how real are threats against us.

I'm just talking about terrorism threats. There are also—obviously most of us who come from California know about the natural threats.

Some say the four seasons of California are fire, floods, earthquakes, and riots, but nonetheless, all of us understand vividly how dangerous our world is.

This hearing explores the failure of the federal government to share critical terrorism-related information with those who need it most, and they're sitting right in front of us, our first responders in state and local law enforcement and their private sector partners.

Just last fall our staff concluded a random survey of police and sheriff's officers across the country to find out what was really going on with information sharing.

One sheriff in North Dakota when asked why we weren't making faster progress had a stunning answer. "I hate to say it," he said, "but 9/11 memories are fading. We simply haven't bled enough to get where we need to be."

Well, I think we shouldn't have to wait for more Americans to be hurt or killed before we get it right.

This subcommittee, on a bipartisan basis, has been focusing on ways to fix how the federal government shares information not only horizontally with its federal partners but vertically with those of you on the front lines.

No one has a monopoly on how to do information sharing, and Washington DC definitely doesn't have all the answers.

I think the greatest hope and most measurable progress is to be found at the state and local levels, and that is why, at the invitation of two capable members sitting to my right and left, we are here in Washington state.

Slowly but surely cities like Seattle, Bellevue, Los Angeles, and others are making real progress in standing up intelligence fusion centers and relaying to the federal government their information needs.

In the view of this subcommittee, we need to make state, local, and tribal sector information needs the driver of federal information sharing efforts not the other way around.

You're the ones who need to identify the information you need, and then that needs to go up the chain, and the federal government, your client, needs to respond to you.

That was the message in the Homeland Security Committee's law enforcement assistance and partnership or LEAP strategy last fall, which some of you are going to address in your testimony.

Law enforcement officers know that to prevent and disrupt a potential attack, they must be full participants in the intelligence cycle, and as some of you pointed out in your testimony, that's the goal, preventing and disrupting not responding.

I am particularly interested in hearing from our witnesses about two ideas in the LEAP strategy, first the creation of a national center for intelligence-led policing. In my view creating such a center makes good sense and will allow locals to learn about the intelligence process as well as the protection of privacy, civil rights, and civil liberties of the people they serve.

Second, the deployment of state and local law enforcement officers to the national counterterrorism center, the NCTC, to work side by side with intelligence analysts.

You may know, and I'm sure the witnesses know, that Congress has passed, in both Houses, a so-called 9/11 bill to implement those recommendations of the 9/11 commission that we have not yet enacted into law.

The Senate and House bills are different, and so a preconference is going out to try to reach agreement and then pass a final version of the bill, which would go to the President.

The 9/11 bill is—at least the House version of it, and we're being effective in persuading the Senate to agree to this, would require the NCTC to include state, local, and tribal law enforcement officers. We've come to that point of view since it's not happening voluntarily, so we're thinking we're going to put a requirement in the law if it doesn't happen before that law is enacted.

The third point I want to make, final point, is that the private sector owns or controls at least 85 percent of this country's critical infrastructure.

Our second panel will include private sector witnesses.

The private sector too needs information that will help inform decisions about how to protect against terrorism.

The newly created national infrastructure advisory council is a positive step forward in addressing private sector concerns about securing facilities. However, the council's recommendations don't appear to be gaining much traction on Capitol Hill.

Local law enforcement agencies like the Seattle police department, on the other hand, have begun to share information with the private sector very successfully, another example of leadership at the local level.

As I mentioned, I was pleased to be invited, but I'm also pleased to join my colleagues, Ranking Member Sheriff Dave Reichert and committee member, Appropriations Committee cardinal, Norm Dicks.

I'm in between a sheriff and a cardinal. It's quite a religious experience.

I'm very pleased also to have read about the progress that Washington state is making.

You may not know that 35 years ago, when we were each 5 years old, Norm and I worked together in the United States Senate. He worked for Senator Magnuson, and I worked for California Senator John Tunney.

We worked there together, although we are from the same political party, at a time when toxic partisanship was not in Washington. It was a better time, but the good news is that Dave and I work together very well, and this subcommittee works on a bipartisan basis.

I haven't—our legislative projects and our hearings have been totally bipartisan, and as far as I'm concerned, that's the way you get the job done, so I'm very pleased to be here with Norm and Dave, the cardinal and the sheriff—maybe a play could be written—and at this point would like to recognize two people in our audience and introduce our first panel.

First the mayor of Bellevue—I think he's still here—Grant Degginger is here, and the Interim Police Chief Linda Pillo is here.

If you want to get the job done right, put a woman in charge, right?

So let me tell you that I'm very excited about our witnesses today, and we'll introduce the first panel, and then you will each testify or summarize your testimony in five minutes.

Ms. HARMAN. Yes, I forgot about Dave Reichert giving his—thank you. Everyone has been pulling at me, and I couldn't figure out what I had said wrong about the mayor.

Let me first yield to the ranking member for an opening statement.

Mr. REICHERT. Thank you, Madam Chair.

The hesitancy is that she knows once I get the microphone, I continue to talk and talk and talk.

I've learned that's what you do in DC is that you grab the microphone and never stop, right, Norm?

Mr. DICKS. Five minute rule in the House.

Mr. REICHERT. So for those of you—and they really go by the five-minute rule.

For those of you who haven't experienced a federal hearing before—I know that the panel has—it's quite an experience back in Washington DC, and it's kind of a formal experience, but usually the members of the committee, we get to pontificate for a while, and then we get to hear the witnesses and their testimony, and we get to ask questions.

Part of the reason we do that is we want to learn as much as we can, and we go back and build good legislation, and, as Jane said, we really have been a committee that has worked well together.

We are a committee that is really focused on protecting this country and protecting our citizens and protecting our community and doing away with that bipartisanship—or that partisanship that you see back in Washington DC, so you'll see this committee really focused on that.

Again, thank you, Madam Chair, and welcome to Washington state, and Norm and I are, of course, good friends, and thanks for coming up from the south end today, Norm, and welcome to the 8th District.

I'm just going to read a prepared statement very quickly.

I would like to welcome, again, the Chairwoman here for this hearing, glad that you were able to make it and thank you for coming to Seattle.

We are all here because we agree that having information flow to and from our first responders is paramount in preventing a future terrorist attack.

However, information sharing is a two-way street. It needs to happen in a partnership based on trust and mutual understanding.

That is the purpose of this hearing today, to better understand how information—information sharing, how those needs are being met and how these relationships can be improved.

Unlike many other major cities across the nation, Seattle is located in close proximity to an international border.

It's home to a number of internationally recognized businesses and combined with the Port of Tacoma has the third largest port as well as the largest ferry system in the nation.

Our region is not new to the threat of terrorism.

Ahmed Rasam is a reminder to us of that threat posed by the border, and the challenges we will face in the upcoming 2010 Vancouver Olympics is real.

Collaboration between federal, state, and local entities is key.

It is clear that in Seattle information sharing has improved dramatically since September 11th, and I was fortunate to be a part of those efforts in the beginning and working with everyone represented today on this panel as their partner in law enforcement here.

I know from past experience that increased collaboration between the federal government and local law enforcement needs to improve more though. We have a lot more work to do.

The private sector as well should be involved. They should be helping us to create a better understanding of potential threats to the Seattle area, and though—and through those partnerships being developed at the Washington joint analytical center, the WAJAC, and FBI, information is flowing directly to those first preventers capable of increasing our level of protection, but it is also clear there is room for improvement.

One of the issues I hear about time and time again is ensuring that the federal funding can be used for analysts in fusion centers, and I know that that's something the chief will touch on today.

The Department of Homeland Security recently allowed state and local entities to use grant funding for analysts, but we are looking to strengthen this law.

While the feds have focused their efforts on improving the security in the nation's most critical infrastructures, it is also essential that the federal government focus on forging new partnerships and improving information sharing, whether these networks be human or cyber.

It is essential that these partnerships and networks include the private sector, especially since private sector owns and operates 85 percent of U.S. critical infrastructure.

Part of the difficulty of the information sharing with the private sector is that the private sector companies are often reluctant to

share information with the federal government. They fear exposure to lawsuits and the loss of competitive advantage.

Given the track record from the Department of Homeland Security protecting information, they are rightly worried.

That is why as part the Department of Homeland Security Authorization Act that passed the House earlier this month, I included a provision to study incentives for the private sector for information sharing.

If a company takes a risk in sharing sensitive data, it is essential that potential benefits outweigh possible costs.

Having some sort of incentives in place could help increase the flow of critical information.

I would like to thank all of our witnesses for being here today and for participating in these two panels, and with that, Madam Chair, I yield.

Ms. HARMAN. Thank you, very much Congressman Reichert.

Ms. HARMAN. Congressman Dicks had the opportunity in his home state to make an opening comment but has chosen to waive, and so I know we'll hear from him shortly.

Mr. DICKS. I would like to hear from the witnesses.

Ms. HARMAN. There you go.

Our first witness, Major General Timothy Lowenberg is the Adjutant General of Washington state where he guides the preparation of Washington Army and Air National Guard citizen soldiers and airmen to respond in times of state and national emergency.

Major General Lowenberg is responsible for formulating, developing, and coordinating all policies, plans, and programs affecting the Army National Guard.

He also serves as chair of the national governors association, homeland security advisors council, and is extremely well known nationally, and it is a pleasure to have you as our witness, sir.

Our second witness, Gil Kerlikowske, is the chief of police for the City of Seattle, a position he has held since August of 2000.

During his 35 years in law enforcement, the chief has served in many distinguished capacities, including as the deputy director of the community-oriented policing services, COPS, at the Department of Justice, the police commissioner in Buffalo, New York, and as a patrol officer in St. Petersburg, Florida, and I do know that you're close friends of the chief and the sheriff in Los Angeles.

Again, it's a pleasure to see you.

Our third witness, David McKay—

Mr. DICKS. John McKay.

Ms. HARMAN. John McKay, thank you.

I'm sorry, I had it down wrong in this transcript.

John McKay was, until recently, the U.S. Attorney for western Washington. He was nominated by President Bush to serve as U.S. Attorney on September 19, 2001, and the United States Senate confirmed his nomination several weeks later.

From 1989 to 1990 Mr. McKay served as a White House fellow where he worked as special assistant to the director of the federal Bureau of Investigation in Washington.

I know you also, as I recall, were president of the legal services corporation in Washington in the late 1990s, a very important as-

signment, I believe, and you are presently visiting professor at the Seattle University school of law.

Our fourth witness, John Batiste, is the chief of Washington state patrol, the largest public safety and law enforcement agency in the state.

Chief Batiste oversees the day-to-day management of the agency's six bureaus: Field operations bureau, fire protection bureau, forensic laboratory services bureau, investigative services, management services, and technical services.

Without objection, each of your full statements will be inserted in the record, and I would ask you each to summarize your statement in five minutes, and I can't see, but is there a timer—over there, so for those—why don't you focus it toward the people who are testifying first, and we're starting with Major General Lowenberg.

STATEMENT OF MAJOR GENERAL TIMOTHY J. LOWENBERG, WASHINGTON MILITARY DEPARTMENT

General LOWENBERG. Thank you, Madam Chair and members of the committee. It's a pleasure to be a member of this distinguished panel with my friends and colleagues with whom I've worked so long and so well.

As noted, I am testifying today as a state official but also as chair of the national governors association of homeland security advisors council.

In fact, I had a national teleconference at 11:00 local to review my testimony with my colleagues from all of the states, and I also appear today as chair of homeland defense and homeland security for the adjutant generals association of the United States.

Let me begin by stating an obvious but critical ground truth acknowledged by the chairwoman, and that is that we are a nation at war, a nation whose communities for the first time in our nation's history are part of the global battle space, and the intent of our adversaries is very clear.

The "Blind Sheik" when he was sentenced for a life term of imprisonment for the 1993 bombings of the World Trade Tower said, and I quote, "God will make America disappear from the surface of the earth as He has made the Soviet Union disappear."

With a lot of great leadership and unity of effort, we have done a number of things to make us safer today than we were when we were attacked in 2001, but we are far from safe.

The 9/11 commission did a laudable job of addressing the spectrum of threats related to al-Qa'ida and what they referred to as ideological movements, but I believe it's also important that we address the spectrum of home-grown terrorism, to that I would add specifically the growing phenomenon of prison radicalization in U.S. prisons, principally in our state prison systems, and these and other domestic threats can only be dealt with by leveraging the vastly superior numbers and "boots on the ground" contacts or our local law enforcement and officials in the private sector as well.

The homeland security advisory council released a report in December of 2004 that went well beyond the 9/11 commission's reports in focusing on the criticality of incorporating these state, tribal, and local intelligence-gathering, intelligence-fusion, and infor-

mation sharing capabilities, and focused on the need for a truly national as opposed to a federal system of intelligence and information sharing.

The LEAP strategy mentioned by the chairwoman I think goes a long way, provides an excellent road map for a true enterprise strategy that would enhance and improve our nation's domestic security.

I know that Chief Kerlikowske is going to comment on the national center for intelligence-led policing and some of the other specification provisions, so I'm not going to spend my limited time doing that, other than to acknowledge that the kinds of activities that support or many times presage domestic terrorist events can best be discerned, interdicted, and prevented when there is a seamless local, tribal, state, and federal intelligence network.

The ground truth is that state intelligence centers have been established almost solely as a result of the initiative and the perseverance of local jurisdictions and states.

There's been tremendous pushback from the very inception.

We were told initially that it wasn't part of the national strategy when then Governor Mitt Romney led the Homeland Security's advisory council's effort on intelligence and information sharing and released their report.

It took us more than a year to get that report through the advisory council, simply to acknowledge the efficacy of state and local intelligence fusion centers.

Once we got that in the fiscal year 2005 grant guidance, we were told that we could hire up to two contract planners to assist the state efforts, but we weren't given the guidelines to enable us to do what we really needed to do, and that was begin to develop a cadre of analysts.

Beginning in fiscal year 2006 we've been authorized to hire analysts but only with grant money limited to the two-year program cycle of the grant, and so as we look at how we fund these efforts at the state and local level, we are restricted to part-time contract employees.

It does not allow us to build a cadre of professional analysts so necessary for national security.

By the way, Madam Chair, you mentioned the NCTC, and we need state and local representation on the NCTC, the national counterterrorism center, that goes beyond one or two fellowship status prisons.

What we really need is a regime in which state and local analysts rotate through the NCTC and federal analysts rotate into the field, so that over a period of time we begin to develop crosspollination personal and professional relationships where fusion center analysts at the various echelons truly have a keen appreciation and understanding of the requirements at the other echelons.

What jeopardizes the operations of state and local intelligence fusion centers in Washington and every other state is the lack of predictable and sustainable federal funding.

We believe, and when I say "we," the Homeland Security advisors for the several states and territories, believes that a multiyear POM cycle for Homeland Security budgeting, much like we do for

the Department of Defense budgeting, is long overdue and would help lay the groundwork for strategic and long-term homeland security planning at all levels of government.

We also believe fervently that the restrictions of DHS information bulletin 235, which limit funding support for its contract intelligence analysts to the two-year performance period, is really not driven by any Congressional authorization or appropriation language and is policy that is off the mark.

If it's not revised, it should be revised by Congress.

Finally, a national as opposed to a federal intelligence center communications architecture needs to be developed and funded, tying together intelligence centers within the states, within intrastate and interstate regions and nationally.

Targeted support from Congress that would allow us to develop this information-operations-sharing database and information system will go a long way to making our country more secure.

Thank you, Madam Chair, for the opportunity to appear before you, and I look forward to your questioning.

Ms. HARMAN. Thank you, General, and I will just point out to you that the legislative fix we have in mind in the 9/11 bill for the NCTC is exactly what you described, so hopefully we will get that very soon.

General LOWENBERG. That will be very welcome.

[The statement of General Lowenberg follows:]

PREPARED STATEMENT OF MAJOR GENERAL TIMOTHY LOWENBERG

Good afternoon, Mr. Chairman and distinguished members of the Committee. For the record, I am Major General Tim Lowenberg, Adjutant General of the State of Washington. I am also Chair of the National Governors Association (NGA) Homeland Security Advisors Council and Chair of Homeland Defense and Homeland Security for the Adjutants General Association of the United States (AGAUS). In addition to my Army and Air National Guard command responsibilities, state law designates the Adjutant General as the state's senior emergency management official and vests in me the responsibility to "administer the comprehensive emergency management program of the state of Washington (RCW 38.52.005).

I wish to emphasize that although I am a federally recognized and U.S. Senate-confirmed Air Force general officer, I appear before you today solely in my capacity as a state official.

We are a Nation at War!

We are a nation at war! That is the "ground truth" that must drive all of our data collection, information sharing and intelligence fusion and risk assessment actions.

We have been under attack since al-Qa'ida operatives prevailed in a decade-long battle against one of the world's two acknowledged "Super Powers" in Afghanistan. Having watched the Soviet Union implode and literally cease to exist within two (2) years of the conclusion of that bloody conflict in 1989, al-Qa'ida began systematically attacking United States interests at home and abroad. The ongoing conflict has already lasted longer than America's involvement in World War II—with no end in sight. More than three thousand U.S. residents perished in the September 11, 2001 attack. Today, all American communities, large and small, are part of a new and frighteningly lethal 21st Century global battle space.

Our adversaries' intentions—and commitment—are manifestly clear. At his sentencing for masterminding the 1993 bombing of the World Trade Towers, Sheik Omar Abdul Rahman (the "Blind Sheik") declared: "God will make America disappear from the surface of the earth, as He has made the Soviet Union disappear!"

We Are Safer Today—But Not Safe

As the Governor's Homeland Security Advisor and Chair of the NGA Homeland Security Advisors Council, I am often asked if we are safer today than we were on

September 11, 200l. In other words, are we safer today than when we were last attacked?

The principal studies and statutory materials I rely upon in responding to this question include the 9/11 Commission Report; the Homeland Security Act of 2002; the Intelligence Reform and Terrorism Prevention Act of 2004; the December 2004 Homeland Security Advisory Council Intelligence and Information Sharing Initiative chaired by then-Governor Mitt Romney; and the 2006 Law Enforcement Assistance and Partnership Strategy. The 9/11 Commission Report reminds us that "Since 9/11, the United States and its allies have killed or captured a majority of al-Qa'ida's leadership; toppled the Taliban, which gave al-Qa'ida sanctuary in Afghanistan; and severely damaged the organization. Yet terrorist attacks continue. Even as we have thwarted attacks, nearly everyone expects they will come. How can this be? The problem is that al-Qa'ida represents an ideological movement, not a finite group of people. It initiates and inspires, even if it no longer directs. —Because of the offensive actions against al-Qa'ida since 9/11, and defensive actions to improve homeland security, we believe we are safer today. But we are not safe."

I concur with this analysis. To the obvious threats posed by al-Qa'ida's "ideological movement", I would add the dangers of home-grown terrorism to include the growing and disturbing phenomenon of U.S. prison radicalization. These domestic threats can only be dealt with by leveraging the vastly superior numbers and "boots on the ground" contacts of state and local law enforcement officials.

To improve domestic security, the 9/11 Commission stressed the importance of *unity of effort* within the intelligence and information sharing community and urged, among many recommendations, targeted intelligence initiatives to create (1) a national counter-terrorism center to unify strategic intelligence and operational planning; (2) a national intelligence director to unify the intelligence community; (3) increased congressional oversight; and (4) establishment of a specialized and integrated national security unit within the FBI.

Subsequent to the 9/11 Commission report, the Homeland Security Advisory Council released a report in December 2004 that focused specifically on the nation's intelligence and information sharing requirements and went even further in recommending:

- Effective prevention efforts must be information-driven and risk-based.
- Federal, state, tribal and local authorities must work together with the private sector to assess threat, vulnerability, risk and consequence.
- State, tribal, local and private entities are now "consumers" of accurate, timely and actionable intelligence.
- The federal government needs to develop a reliable and organized conduit for providing information to state, tribes, and localities.
- The federal government should emphasize providing current and actionable unclassified information.
- ***The collectors of intelligence; state, tribal and local entities are now partners with the federal intelligence community. ****
- The federal government should take steps to ensure domestic intelligence/information activities are carried out in a consistent fashion.
- ***State, tribal and local governments need to collect, analyze, disseminate and use intelligence and information as part of their day-to-day operations. ****
- DHS should gather and share best practices.
- ***Statewide intelligence/information fusion centers should be an important part of national intelligence/information sharing efforts. ****
- ***Each state should establish an information center that serves as a 24/7 "all-source," multi-disciplinary, information fusion center. ****

* (emphasis added)

Two years after release of the Homeland Security Advisory Council report, the House Committee on Homeland Security proffered additional and more precisely focused recommendations in its Law Enforcement Assistance and Partnership (LEAP) Strategy. I applaud the House Committee's analysis and concur with many of the LEAP Strategy recommendations including establishing a national center for intelligence-led policing; establishing a law-enforcement presence overseas; creating intelligence fusion centers at or near our borders; supporting grant programs to assist local law enforcement education and teaming; enhancing vertical information sharing between levels of law enforcement; assuring timely accessible security clearances for law enforcement; and continual surveying efforts to provide feedback on intelligence system effectiveness. If authorized and funded, these initiatives would enhance unity of effort and fundamentally improve our nation's domestic security.

To date, however, most of the attention and funding for these and other initiatives have been focused at the federal level. While continuously improving federal inter-

agency operations, we must also be mindful that terrorist attacks and criminal activities that support terrorist activities occur in local communities and local citizens are the primary victims. Unless and until the federal government also supports and funds a national strategy of state and local counter-terrorism capacity building, homeland security will continue to be an illusive goal.

Federal-Centric First Steps

In 2003 the Terrorism Threat Integration Center (TTIC) was formed to provide a comprehensive assessment of potential terrorist threats to U.S. interests. The TTIC included the Department of Homeland Security, the FBI's Counterterrorism Division, the Central Intelligence Agency's Counterterrorist Center, the Department of Defense and other U.S. Government agencies. The Intelligence Reform and Terrorism Prevention Act of 2004 renamed the TTIC the National Counterterrorism Center (NCTC) and placed it under the control of the United States Director of National Intelligence (DNI). The NCTC vision statement calls for it to serve as the nation's center of excellence for counterterrorism and to eliminate the threat of terrorism through integrated, dedicated and disciplined strategic operational planning and counterterrorism intelligence. One of its stated objectives is to operate as a partnership of organizations including: the Central Intelligence Agency; the Department of Justice/Federal Bureau of Investigation; the Departments of State, Defense, and Homeland Security; and other entities that provide unique expertise such as the Departments of Energy, Treasury, Agriculture, Transportation, and Health and Human Services; the Nuclear Regulatory Commission; and the US Capitol Hill Police.

While this vision, purpose, and strategy are prudent and highly important, I mention the creation of the TTIC and NCTC as an illustration of the federal-centric nature of many of our initial homeland security initiatives. Without diminishing the importance of these and other federal government actions, they must be part of a larger enterprise strategy of federal-state-tribal-local capacity building, especially in the areas of intelligence fusion and information sharing. As DHS moves forward with efforts to create uniform information sharing guidelines, it is imperative that they have a better understanding of state operations and how state, tribal and local operations can enhance our overall national intelligence system. State intelligence fusion centers have had to be built almost exclusively through state and local perseverance, not as a result of any federal encouragement or federally-supported national strategy. Even after release of the Homeland Security Advisory Council's Intelligence and Information Sharing Initiative report touting the national security benefits of state-tribal-local intelligence fusion centers, financial support from DHS and OMB was not forthcoming. Only after a substantial number of states established such centers and others were clearly in the process of doing the same did DHS and OMB belatedly begin providing limited funding support for these state and local operations.

With American communities at the heart of the new 21st Century battle space, we cannot afford to "manage" the consequences of future terrorist attacks. We must be able to detect, deter, intercept and prevent such attacks from occurring. That can only be done through the systematic gathering, assessment, distillation and dissemination of actionable intelligence. The LEAP report accurately notes that intelligence analysis has heretofore been the near-exclusive domain of the federal government and that we have been slow to recognize that local, state, and tribal law enforcement professionals, if properly resourced, are our nation's true "eyes and ears" and can substantially enhance our nation's security.

When planes were flown into buildings on September 11, 2001 it was the brave men and women of local police and fire departments who heroically responded. That same sense of urgency and commitment exists today in our state, tribal and local intelligence fusion centers.

—Enhancing State and Local Intelligence Fusion Capacity—

Creating a "National" Intelligence System that Makes our Nation Safer!

Capitalizing on an All-Crimes Approach

To develop a broader intelligence sharing system, additional information, that is to say information other than that which has a clear nexus to terrorism, must be considered. To that end, the LEAP report observed:

Everyday, police and sheriffs' officers collect millions of pieces of information during the course of their work—the kind of information that, if properly analyzed and

integrated, can form the basis of highly informative law enforcement intelligence reports. That is what "intelligence-led policing" or ILP is all about.

Another proponent of ILP, Michael Downing, Commander of the Los Angeles Police Department's Counter-Terrorism/Criminal Intelligence Bureau, has opined:

The success and understanding of community based policing philosophies and community based government practice [has] set the stage for local, state, and federal law enforcement partners to construct the building blocks for shared and fused intelligence that will prevent, deter, disrupt, and interdict planned terrorist acts targeting America. This intelligence model of policing should be robust enough to incorporate an "all-crimes, all-hazards" approach, resisting terrorism as well as crime and disorder.

The state of Washington has firmly embraced an all-crimes approach to the collection, analysis and dissemination of intelligence information. The State's fusion center, known as the Washington Joint Analytical Center or WAJAC, regularly dispenses actionable intelligence and Be-On-the-Look Out (BOLO) information related to terrorism as well as a variety of topics including missing children, stalking suspects, counter-drug and narcotics interdiction missions, auto-theft rings, and organized gangs.

This kind of information can only become fully actionable when state, tribal and local fusion centers are linked together by consistent communications architecture within states and throughout the nation. A national—as opposed to a federal—intelligence center information operations (IO) strategy would facilitate the horizontal and vertical sharing of "real time" classified and law enforcement sensitive information.

We should also leverage the skills and capabilities of trained and experienced analysts and subject matter experts from our state prison systems and from non-law enforcement disciplines such as the Army and Air National Guard and Public Health.

The Need for Predictable and Sustainable Federal Funding

Above all else, however, what jeopardizes the operations of state and local intelligence fusion centers in Washington and all other states is the lack of predictable and sustainable funding. Current federal grant guidelines (Information Bulletin—IB235) authorize funding support for intelligence analysts for only the 2 year performance period of the fiscal year 2006 UASI and LETPP programs.

Fiscal Year 2006 Grant Guidance (pages 33–34, 83, 89):

"Furthermore, costs associated with hiring new intelligence analysts are allowable only for the period of performance of the fiscal year 2006 UASI and LETPP programs. Upon close-out of the fiscal year 2006 grants, States and Urban Areas shall be responsible for supporting the sustainment costs for those intelligence analysts."

Fiscal year 2007 HSGP Grant Guidance (pages 26 and B–1):

"Costs associated with hiring new intelligence analysts are allowable for only two years, after which States and Urban Areas shall be responsible for supporting the sustainment costs for those intelligence analysts."

Although there are no references to intelligence analysts in the congressional appropriation bills, the Department of Homeland Security, as a matter of discretion and policy, has issued IB235 which tracks both grant guidelines and applies the two year limitation to both years' funding. These limitations, coupled with the overall uncertainty and unpredictability of federal grant funding, create continuous staff turnover and prevent state and local fusion centers from developing a cadre of experienced career analysts. The federal government wouldn't think of contracting out its Intelligence functions, yet the DHS policy essentially forces state and territorial governments to rely upon contract personnel hired for only a 2-year grant performance period. States are predictably unable to recruit and retain skilled personnel when federal grant guidelines accommodate only short-term, "temporary" contractor assistance.

Synchronizing State and Federal Information Sharing and Intelligence Analysis

Washington State's proximity to the Canadian land border, coupled with our proximity to Puget Sound and the Pacific Ocean, provide ample air, land and maritime routes of illegal entry for those who would do us harm. These geographic vulnerabilities substantially increase the risk of a terrorist attack especially when viewed against the backdrop of the world "stage" that will be presented to terrorist cells by events such as the 2009 World Police and Fire Games and the 2010 Winter Olympics and Paralympics. Many of these events will be held in and near Van-

couver, British Columbia at venues within 35 miles of Washington State communities. If domestic or transnational terrorists were to plot an attack in conjunction with these international events, it is likely that pre-operation planning and surveillance will be conducted from within the state of Washington. Given al-Qa'ida's modus operandi, such planning might even be occurring in our region today.

Developing a closer, more disciplined information sharing relationship between local, state, and tribal law enforcement and Customs and Border Patrol (CBP), Immigration and Customs Enforcement (ICE) and other federal agency colleagues would substantially enhance our collective situational awareness. In this regard, I concur with the LEAP report's observation that "in order to better secure the homeland, the Department [of Homeland Security] must partner more effectively with state, local, and tribal law enforcement agencies in our nation's border communities—the 'force multipliers' at our own frontiers."

David Carter, Professor and Director of Michigan State University's School of Criminal Justice, noted in the LEAP report:

The borders of the U.S. are replete with small state, local, and tribal law enforcement agencies. Officers in those agencies know the people in their communities and the character of life on the border and readily recognize when there are anomalies. Yet, they rarely report this information and even more rarely are asked. This is valuable data that may often times help fusion center analysts and the federal Intelligence Community complete the threat puzzle.

Fortunately, Washington State has benefited from a close relationship with our federal border partners. Specifically, Thomas Hardy, Director of Field Operations for the Seattle CBP Field Office, and his staff have been invaluable collaborators, particularly as we have worked together on preparing for the 2010 Winter Olympics.

Washington's local police agencies have also benefited from a high level of collaboration with our federal agency partners. In the LEAP report, Ferry County (WA) Sheriff Peter Warner emphasized:

> We rely on Border Patrol agents in my jurisdiction for information about what's going on at the border, and I know them personally. We frankly need more Border Patrol agents—and more resources to hire additional police and sheriffs' officers—in order to meet the threat of terrorism at the border.

I concur with Sheriff Warner and encourage the members of this Committee and your fellow members of Congress to appropriate funding for additional human and technological resources at the federal *and at state and local levels—with special and targeted support for state and local intelligence fusion center operations*—to help ensure the air, land and maritime routes of access to our country are secure.

Conclusion

We are a nation at war. We are confronted by daunting and unprecedented domestic security risks. Our ability to detect, deter, dissuade and prevent future terrorist attacks is directly tied to our ability to analyze all-crimes intelligence in adequately funded and staffed state and local intelligence fusion centers and in collectively sharing that information between and among members of the local-tribal-state-federal intelligence community. A federal-centric intelligence system will not allow us to meet the threats now confronting our nation nor will it enable us to effectively respond to or recover from future terrorist attacks. Our homeland will be secure only when members of local, tribal, state and federal law enforcement communities and other emergency responders have the information and resources they need on a daily basis to make sound decisions about transnational and domestic terrorist threats.

Thank you for the opportunity to appear before you today. I look forward to your questions.

Ms. HARMAN. Chief Kerlikowske, please summarize your testimony in five minutes.

STATEMENT OF R. GIL KERLIKOWSKE, CHIEF, SEATTLE POLICE DEPARTMENT

Chief Kerlikowske. Thank you, Committee Chair Harman and Congressman Dicks, Congressman Reichert. Thanks very much for inviting me to share observations with you on the very important topic of information sharing between the public and private sectors as it relates to homeland security.

I'm going to sketch for you the state of intelligence fusion and homeland security from the vantage point of a local police chief,

and I want to address the following two areas: The nature of the current obstacles to the creation of an integrated system of intelligence fusion, including private sector participation; and some proposed solutions for removing those impediments and improving the information sharing, in particular some of the promising initiatives contained in the LEAP report which myself and my colleagues have been very impressed with.

The essential concept of intelligence fusion, which is in several different national guidelines, fusion center guidelines, et cetera, involves the systematic collection, analysis, and dissemination of information through an inclusive process, involving the full engagement of all of the key stakeholders, and without the participation of the private sector, which as you mentioned, Madam Chair, holds, manages and controls over 85 percent of the critical information infrastructure in the nation, it is hard to contemplate that we are going to be able to achieve that objective.

Realization of such private/public partnership is predicated upon though having a system upon which we are going to all participate, and this is the dilemma that vexes my colleagues and the major city chiefs, that is the organization of the 56 largest police and sheriff's departments in the United States and Canada and where I currently serve as vice president.

We consider increased engagement of participation by the private sector in homeland security to be among one of our highest priorities.

Unfortunately, our individual ability to collect and create intelligence fusion centers has been limited, at best.

Two of the major impediments: First, we remain tethered to the federally centered vision of intelligence information based on the Cold War "bottom up" type of system. Security clearances are difficult and time-consuming procedures for obtaining access to equipment, are convoluted and unnecessary, and the sharing of vast categories of information is prohibited unless it is brokered by DOJ or DHS.

Second, the restrictions on the use of funds to support homeland security, which the General mentioned and I believe Chief Batiste will mention also, the potential solutions are contained in the LEAP report.

One is, of course, what you had mentioned earlier, the proposal to establish a center for intelligence-led policing.

We are doing this, as the sheriff or Congressman Reichert knows, across the country and looking at best practices in collaborating and working together.

Having this federally located system and funded system would go a long way to that.

The foreign liaison officer against terrorism program—you have great acronyms, by the way, for this. Very well done.

Ms. HARMAN. Give our staff the credit.

Chief Kerlikowske. The FLOAT program—what an ability in this global issue to be able to have local law enforcement understand and obtain knowledge in foreign countries, something that we could not, unless you are New York City, afford to do, the proposal to reform and streamline the process for obtaining security clearances.

In Seattle we have a convergence of the circumstances that have created the ideal environment for information sharing, and that is some of the things that we can accomplish in the city, and I very much appreciate the support that we've had from our own local members.

Right after 9/11 we were able to reach out to the Muslim community and through a joint letter signed by, at that time, United States Attorney John McKay and myself, we notified every police agency in the state of Washington how they could be helpful in reducing fear and increasing cooperation and communication in those communities.

We participated in TOPOFF, the first federally centered exercise against terrorism after 9/11.

Under John McKay's leadership, the Puget Sound region was the first to operationalize Linx, the law enforcement system for data coordination, and we have been working very hard at a regional fusion center in conjunction with our state fusion center, WAJAC.

Our areas of interest converged and create substantial opportunities for expanded collaboration. No one knows the strengths and vulnerabilities of these critical facilities better than the locals do.

What I suggest is that we seek the kind of enduring dependable relationship we have in Seattle with leaders like Al Clise and Richard Stevenson of Clise Properties. That is a foundation of trust and cooperation and relationships that make sure that we are going to protect the critical infrastructure in the private sector to the very best of our ability.

Thank you.

Ms. HARMAN. Thank you very much, Chief.

[The statement of Chief Kerlikowske follows:]

PREPARED STATEMENT OF CHIEF R. GIL KERLIKOWSKE

Committee Chair Harmon, Congressman Dicks and Congressman Reichert, thank you for inviting me to share my observations with you on the important topic of information sharing between the public and private sectors as it relates to homeland security.

To address the central question of this hearing—How do we build a partnership between the public and private sectors to share information relevant to homeland security?—requires an analysis, first, of the status of homeland security intelligence efforts and systems to date. This is because we cannot share information and intelligence that we don't have. Moreover, it would be premature to undertake an expansion of information sharing if the infrastructure of intelligence fusion is inadequate or incomplete.

In the brief time I have today, then, I will attempt to sketch for you the state of intelligence fusion in support of homeland security, from the vantage point of a local police chief, by addressing the following:

- the nature of current obstacles to the creation of integrated systems of intelligence fusion, including private sector participation; and
- proposed solutions for removing these impediments and improving the information sharing environment, in particular, some of the promising initiatives contained in the "Law Enforcement Assistance and Partnership Strategy", or LEAP report.

I will conclude my testimony with some observations aimed at reinforcing the importance of public private partnerships, and why I am optimistic that we will achieve success to meet that priority.

Obstacles to creating integrated intelligence fusion.

The essential concept of intelligence fusion—as defined by DHS in both National Criminal Justice Information Sharing Plan (NCISP) and the NIJ-Global Justice Initiative "Fusion Center Guidelines" document they adopted—involves the systematic collection, analysis and dissemination of information through an inclusive process, involving the full engagement of all relevant stakeholders. Without the participation

of the private sector, which holds, manages and controls over 85% of the critical information infrastructure of the nation, it is hard to contemplate achievement of this objective.

Realization of such a private/public sector partnership, however, is predicated upon having a system or process within which to participate. This is the dilemma which has vexed my colleagues in the Major City Chiefs organization, which comprises the 56 largest metropolitan police agencies in the US and Canada, and where I currently serve as vice-president. We consider the increased engagement and participation by the private sector in homeland security to be among our highest priorities. Unfortunately, our individual and collective progress to create intelligence fusion systems or centers that have the capacity to integrate private sector participation has been limited, at best.

Two major impediments have contributed to this reality:

First, we remain tethered to the federally centered vision of intelligence information management. Developed during the Cold War, this vision remains stubbornly resistant to change. For all the stated commitment to derive intelligence requirements and priorities from the "bottom up"—which I interpret to mean from the front lines of local law enforcement—many decisions still originate from somewhere inside the beltway, and specifically within DHS and the FBI. This reality finds confirmation in many ways. Security clearances are difficult for many in law enforcement to obtain in a timely fashion.

- Procedures for obtaining access, equipment or support are often convoluted, tortuous and unnecessary.
- The sharing of vast categories of information is prohibited unless brokered by the FBI, in particular as relates to foreign counter-intelligence. (As a police chief of the 19th largest city in the nation, and in possession of a top secret clearance, by law I cannot set foot unescorted in the NCTC, let alone have direct access to even the most benign information)
- And while there are some noteworthy and commendable fusion centers and systems around the country (I am thinking here of Los Angeles–Los Angeles County, Arizona and Massachusetts, to name a few), the vast majority of intelligence management remains centered in the traditional JTTF–FIG structure, almost six years after 9/11.

Second, the restrictions on the use of funds to support homeland security initiatives virtually assure that our progress will be limited. In particular, the UASI prohibitions concerning the hiring of sworn law enforcement personnel contradict an order of priority that every chief of police knows by heart: It is people who solve crimes and prevent terrorism, not buildings and equipment.

Potential solutions for improving the information-sharing environment.

My purpose in making the above observations is not to itemize grievances, but rather to join with you in finding solutions. Just as it is fair to say that many of us in the local law enforcement community have been frustrated by certain unnecessary, and sometimes mysterious, impediments to our progress relating to homeland security, it is equally fair to say that we have come a long way since 9/11, and that the nation is, on balance, safer and more prepared than we have been in the past. And we are all keenly interested in continuing the progress that we have jointly achieved. This brings me to comment on certain of the promising initiatives contained in the LEAP report. Specifically, I wish to lend my voice in support of the following initiatives outlined in this laudable, strategic document:

First, the proposal to establish a "center" for intelligence-led policing. This, to me, makes a lot of sense. From my vantage, there does not appear to be sufficient attention paid to creating a unified approach to the overall concept of intelligence-driven policing on an all-crimes basis, nor is there sufficient focus upon the strategic or civil liberties implications of police deployment based upon actionable information. The opportunity to evaluate successful models and develop standards and guidelines on a national level would meet a great need. This being said, the concept of a national center must be more than just about building another big box, of course, and must be designed based upon the concepts I discussed earlier. Fundamentally, the full participation of local law enforcement is critical to the success of such an initiative. Perhaps there would be a place in such a center or system for the private sector, as well.

Second, the "Foreign Liaison Officers Against Terrorism (FLOAT) Grant Program" would go a long way toward expanding both the knowledge base and the preparedness capacity of local, state and tribal law enforcement. In a real sense, a program of this kind directly confronts the preclusion of local law enforcement involvement in the categories of intelligence that I spoke of earlier. This program would open the eyes of local law enforcement to understanding this issue and create a knowledge base around terrorism and international crime that is presently lacking. Remember that most police agencies have trouble talking to their next-door neighbors, let alone

communicating across international borders. This is an extremely worthwhile component of LEAP.

Third, the proposal to establish and fund a "Vertical Intelligence Terrorism Analysis Link (VITAL)" is directly on point to confront the current restrictions on local law enforcement access to relevant foreign intelligence data. This proposal strikes an appropriate middle ground between the integration of local law enforcement in foreign counterintelligence missions—which, except in extreme cases, I do not advocate—and allowing appropriate access to information that links to threats directed at the communities we police. Like the FLOAT program, this proposal is based upon a mature recognition that for 99% of the populous, their homeland is not inside the beltway, but is instead the city, town or unincorporated county where they reside; and their homeland defenders are the local police officers and sheriff's deputies who live and work in those same cities and towns.

Fourth, the proposal to reform and streamline the process of obtaining security clearances will find few—if any—detractors among law enforcement executives. Both the goal of the initiative and recognition of the priority of this need are long overdue.

There are many other laudable proposals described in the LEAP strategy document, including the need to strengthen border intelligence capacity through the creation of a specific focus on US border intelligence fusion, and I do not want my failure to mention them to suggest a lack of support.

In my time remaining, though, I want *to return to the issue of creating greater opportunities for public-private information sharing.*

As I stated earlier, the need to understand the challenges that inhere in our commitment to create systems of intelligence fusion is a prerequisite to any meaningful discussion of public-private information sharing. I have spent some time describing both the limitations and promising alternatives to the current picture of intelligence fusion confronting local law enforcement, for the reason that meaningful partnerships are founded upon meaningful systems that provide timely and relevant information. In other words, we must build a strong house if we intend to invite our private sector partners to share floor space. With that, I turn how to the issue of creating greater opportunities for public-private information sharing.

When I consider the current status of intelligence sharing between local law enforcement and the private sector, I must first observe that the quality and frequency of the exchange of information remains more a matter of personal relationships and individual initiatives than a well-organized, reliable system of intelligence fusion that includes private sector representatives as full partners. As happens frequently in this profession, whom we know and have worked with in the past defines the boundaries of engagement, particularly as concerns sensitive or classified information. And while public-private partnerships remain a priority in the design and implementation of intelligence fusion, there remain few examples of the kind of fully-integrated, systematic collaboration with the private sector that state and local public safety leaders acknowledge as a vital component of comprehensive intelligence management. The need for this cooperation is evidenced in the Pulitzer Prize winning book, *Looming Tower.*

This is not to suggest that the model of personal, relationship-based engagement and collaboration cannot meet our objectives for intelligence sharing in the short term. At the local level, relationships between police and community have been a force multiplier, and have been shown in many cases to prevent or reduce crime. In a real sense, it is precisely these relationships which make a system of public-private collaboration even possible.

In Seattle, for example, we have a convergence of both circumstances and initiatives that create an ideal environment for information sharing. Our business, minority and neighborhood communities have a long and proud tradition of civic participation and contribution. Almost twenty years ago, the Seattle Police Department established a structure of precinct level advisory councils, which were so successful that they were expanded to include specific councils representing communities of color, sexual minorities, private security companies and human service providers.

Some examples of how this information environment has been of value in the context of homeland security are, as follows:

- Immediately after 9/11, our outreach to the local Muslim community addressed practical fears and concerns, and at the same time showed the world that humanity has many diverse faces and beliefs.
- The City elected to participate in TOPOFF 2, the first national terrorism exercise after 9/11, which created new partnerships and brought many diverse people and interests together in a real time exercise to test our preparedness.
- We were able to create a Seattle Police Foundation, comprised of many of the city's most important and civic-minded business and community leaders.

• Under the leadership and commendable commitment of US Attorney John McKay, the Puget Sound region was the first to operationalize the "LinX" (Law Enforcement Information Exchange) data coordination system.
• And we are in the process of designing and implementing a regional fusion center which seeks to integrate, to the greatest extent possible, private sector participation.

The City of Seattle and the Puget Sound region—like many communities across the nation—has the capacity to transform our time-tested, profound personal relationships within the private sector into a system and structure of regular information sharing. So in thinking about the potential for public-private intelligence sharing, I believe it is not so much a matter of will as a matter of structure and design, and of overcoming impediments that frustrate our shared commitment to collaborate. The real key to this transformation, however, consists of law enforcement consciously and purposefully broadening its engagement with the private sector, much in the same way we have asked DHS to expand the scope of their engagement and partnership with local law enforcement.

One area where our interests converge and create substantial opportunities for expanded collaboration is in the analysis of critical infrastructure. No one knows the strengths and vulnerabilities of the critical facilities we seek to protect better than their owners and staff. Another is in the area of integrated communications, to include the possibility of interoperability.

What I suggest we seek is the kind of enduring, dependable relationship we in Seattle have with leaders like Al Clise and Richard Stevenson of Clise Properties. You will hear testimony today from Richard about how our longstanding professional friendship has been the basis for sharing information about critical infrastructure strengths and vulnerabilities, and has enhanced the capabilities of both the Seattle Police Department and Clise Properties to prevent, detect and respond to threats to those private sector holdings. For obvious reasons, neither Richard nor the Seattle Police Department will disclose any details about this instance of collaboration. The point is that these types of candid, inclusive partnerships are eminently possible. They are founded upon trust, confidence, and mutual respect. They can, and should be, the rule, rather than the exception.

While much work remains, not the least of which involves further development of the infrastructure of intelligence fusion at the local, state and tribal level, it is clear that the potential for public and private sector collaboration and information sharing is significant. We've seen it in Seattle. It is possible in every community in this nation. And it is on this note of optimism that I will close and take any questions you may have.

Ms. HARMAN. Mr. McKay.

STATEMENT OF JOHN McKAY, FORMER U.S. ATTORNEY

Mr. MCKAY. Chair, thank you very much. I appreciate the opportunity to be here as a former United States attorney and a lowly law professor at Seattle University Law School. I thank you very much.

I apologize for being late. I don't know if Madam Chair is aware that we lost a real leader last night, Norm Maleng, and Norm was a close friend of mine and I know of many others here, and we will miss him tremendously, a national leader in deterrent sentencing and programs constructed toward violence against women, many other tremendous services over his 30 years as the elected prosecutor here, and I will miss him terribly.

I wanted to talk for a moment about the role of the federal government in building regional law enforcement sharing systems, and I think we need to distinguish for a moment between fusion centers, which are important because they bring persons together, and bringing the data together, the records together that contain information of crimes.

I think that most law enforcement recognize that while intelligence is incredibly valuable in the war on terror, it may be more important to know what each other knows about crime in our re-

gion, and amazingly we today, in most places in the United States, do not routinely share law enforcement records with each other.

In a world in which we can go online and Google information from all over the world, law enforcement is not capable today, in most places, of finding out what federal agencies, state agencies, and local agencies know about individuals who have been arrested or convicted of crimes; in particular, relating to investigative records which contain full text information about crimes that have occurred and which could be the basis for criminal conspiracies or even terrorist conspiracies.

Madam Chair, we do not do a good job of creating those regional systems.

The individuals on this panel are among some of the very best leaders in law enforcement in the United States, I believe, in creating the governance behind the first Linx system which was operational here in the state of Washington and to include the gentleman to your right, Congressman Reichert, our sheriff here in King County who along with the individuals on this panel with me, including General Lowenberg, have been tremendously helpful in creating the governance necessary to establish a system in which federal, state, and local records reside.

It sounds easy. The public thinks we have it. We do not have this capability, other than a very few places around the United States.

I've set some of those out in my prepared remarks and won't repeat them here.

I do believe that the federal government has an incredibly important role, and it begins with acknowledging what the Chair has said and what Congressman Reichert has said, and that is that local knowledge about crime and local data concerning past crimes and current investigations are in many ways more important than information that the federal government brings to the table.

Yet, it is not possible among the more than 200 law enforcement agencies in the state of Washington, for example, to ask each of them to create a piece of a system that will result in that Google capability that we really do seek.

That means the federal government has to assist in funding. It has to assist in providing the forum for the government structure that will bring those many different police organizations together, all with different civilian supervision at the local, state, and federal level.

That's what the Linx system is, and I'm not here to sell Linx. Linx is owned by the government. It's owned by the Department of Defense.

Some have really maliciously said that Linx is somehow a proprietary system. It isn't.

The key elements of Linx are the ability to search databases that are under the control and supervised by civilian authorities over law enforcement, and I'm very proud of what has been created here.

I'm also terribly disappointed in the Department of Justice in not pursuing the pilot programs that Linx has so successfully launched in a number of places around the country, and I would ask really this subcommittee to consider this question.

I don't believe that anyone in the federal government is responsible for building these systems. We propose an interdepartmental partnership with the United States attorneys between Homeland Security, the Department of Defense, and the Department of Justice.

We believe we had an arrangement to do that. It has not occurred, and I believe that is why when you peel aside the rhetoric and all the nice words, very little law enforcement information sharing is occurring among state, federal, and local partners.

Partnership is the key. We built trust here. We know it can be done, and I'm certainly looking forward to taking any questions that you may have.

Ms. HARMAN. Thank you very much.

[The statement of Mr. McKay follows:]

PREPARED STATEMENT OF JOHN MCKAY

Good afternoon Madam Chair and members of the Homeland Security Subcommittee on Intelligence, Information Sharing and Terrorism Risk Assessment. I am John McKay, the former United States Attorney for the Western District of Washington. I am currently Visiting Professor of Law, Seattle University School of Law. I am pleased to appear before you to present information regarding "Building a Partnership Strategy: Improving Information Sharing with Local and State Law Enforcement and the Private Sector".

It has been my distinct pleasure to serve the citizens of the State of Washington and the Department of Justice as the United States Attorney for the Western District of Washington from 2001 to 2007, when I resigned along with a number of my colleagues from around the country. I was honored to serve with professional men and women in the United States Attorney's Office in Seattle and Tacoma, and with the many extraordinary professional law enforcement personnel from the various local, county, state, tribal and federal law enforcement agencies throughout the State of Washington and around the United States.

One of my most rewarding experiences while serving as the U.S. Attorney was to help lead the development of an extremely effective law enforcement information sharing effort known as the Law Enforcement Information Exchange (LInX). I first became involved in the development of a program to enhance information sharing among law enforcement agencies following the tragic events of September 11, 2001. It soon became apparent after that fateful day that an extraordinary effort would be required to improve information sharing among law enforcement agencies at all governmental levels if we were to be successful in mitigating another devastating terrorist attack on our homeland. As the U.S. Attorney in Seattle, I sought to facilitate the development of an effective information sharing strategy among scores of law enforcement agencies to both mitigate another terrorist attack, and effectively combat rising organized crime in my district.

In early 2002, I was invited to attend a pilot program sponsored by the FBI in St. Louis, Missouri. This program, knows as the Gateway initiative, was an effort by the FBI to demonstrate that local, county, state and federal law enforcement agencies could effectively break down the cultural barriers and obstacles to information sharing, and develop a cost effective technology among their disparate information management systems. During the demonstration of this program, I met with Executive Assistant Director Dale Watson of the FBI, Director David Brant of the U.S. Naval Criminal Investigative Service, and a variety of other U.S. Attorneys to discuss a strategy to expand the Gateway initiative outside of the St. Louis area.

The Puget Sound area of Washington State serves as a vital homeport to the strategic resources of the United States Navy. We have nuclear powered aircraft carriers, ballistic missile submarines and a large civilian and military workforce which are strategic assets in the defense of our country in the Pacific, and which have played a vital role in our military response in both Afghanistan and Iraq. The U.S. Naval Criminal Investigative Service is responsible to provide felony criminal investigative, counterintelligence and counterterrorism support to the Department of the Navy, and to the strategic assets in the Western District of Washington. Following my positive impression of the FBI Gateway Program, I approached Director Mueller and Director Brant to consider a law enforcement information sharing pilot program in my district to enhance our law enforcement and counterterrorism strategies.

The Naval Criminal Investigative Service (NCIS) eagerly accepted my request, and then Director Brant devoted resources to develop what has come to be known as the LInX program. This is more than a technology project; it is in fact a law enforcement and counterterrorism operational capability. The LInX effort in Seattle began with the effective organization of senior law enforcement executives, to include Chiefs of Police, Sheriffs and Special Agents-in–Charge from thirteen critical agencies. NCIS provided the funding to develop the technology to permit the electronic sharing of law enforcement records, to include criminal incident data, traffic summons, computer assisted display (CAD) data, criminal arrest histories and other law enforcement records that are legally retained and shareable by and among these law enforcement agencies. NCIS also provided resources to assist me in formally organizing the leadership of these law enforcement agencies who actually owned and were responsible for the collection of this data. We formed a LInX Board of Governance, which was comprised of this executive level leadership of local, county, state and federal agencies. My office provided direct legal oversight of this program to ensure that all federal guidelines, to include the Federal Privacy Act was complied with in the development of this program.

The NCIS simultaneously initiated LInX Programs in other geographical areas vitally important to the Department of the Navy, and sought to enhance their criminal investigative and force protection support to the Navy through the enhancement of information sharing with regional law enforcement agencies. NCIS developed LInX projects in the Hampton Roads area of Virginia, the Gulf Coast of Texas, Hawaii, Northeast Florida and Southeast Georgia, the National Capital Region of Washington, DC and in New Mexico. In each of these regions, the local United States Attorney was personally involved in the oversight and participation of the LInX project. From 2003–2006 we expanded the Northwest LInX project to include more than one hundred fifty (150) agencies throughout the State of Washington, and most recently to include the Portland, Oregon Police Bureau, which includes seventeen local and county agencies. I believe in total, the LInX Program, now deployed to seven regions throughout the United States, has developed an effective law enforcement information sharing effort with more than 350 agencies.

Throughout my involvement with the LInX Program, I had the opportunity to meet frequently with leaders in Washington, DC, to include the Secretary of the Navy, the Deputy Secretary of Defense, the Deputy Attorney General of the United States and the Deputy Secretary of Homeland Security. In partnership with the Director of NCIS, I offered that LInX has fostered an extremely harmonious environment among law enforcement leaders in the Northwest, bringing them together to plot a strategy for effective information sharing. We successfully overcame those artificial barriers between agencies, which had become a part of the law enforcement culture prior to the events of September 11, 2001. More importantly, with the direction of these law enforcement leaders and their operational personnel, NCIS developed a technical solution for the sharing of electronic data that directly led to law enforcement successes in my District. I received reports from virtually all agencies involved in this effort that their personnel had solved criminal investigations that previously would not have been solved, or would have required extensive resources to pursue.

The LInX Program allowed each participating agency's law enforcement personnel to search and retrieve law enforcement records of other jurisdictions within the State of Washington. In addition, the Department of Justice joined the LInX Program in Washington, by developing a linkage to the DOJ Regional Data Exchange (R–DEX) program, which is an effort to share information between FBI, DEA, AFT, USMS and BOP. For the first time in the profession of law enforcement, detectives from Seattle to Spokane were able to share criminal files with each other, and they were able to query the DOJ criminal investigative components, and determine if any of those agencies had a file of interest to the local agencies.

Unique to the LInX system is the ability to conduct a comprehensive search of law enforcement records, retrieve both structure data and full text investigative narratives, to literally connect the dots to a crime. Most important to me from a strategic standpoint, was the ability of LInX to offer insight into crime committed at the local level, which could be a precursor to a future terrorist attack, or a terrorist support network. These are the dots that could not be connected prior to 9/11. We have developed a system, and a regional organizational structure of law enforcement leaders, which, if implemented on a national scale, could likely prevent the next terrorist attack on our country. Law enforcement information sharing should have the following characteristics:

- The system should include *all the legally shareable data* maintained in the record systems of each participating agency. Access controls must be included to protect sensitive information from widespread or premature dissemination.

- The system must permit partners full access to the relevant documents.
- The system must provide a technical analytical capability to "connect the dots", by linking all variables associated with a subject and instantly providing a composite picture for the investigator.
- The system must meet the security standards of the federal law enforcement agencies.

I am convinced that the elements of the LInX program, and all of the standards that it embodies should be developed by the federal government on a national scale, building on the experience here and in the other NICIS funded pilots.

Deputy Secretary of Defense Gordon England proposed to Deputy Attorney General Paul McNulty and Deputy Secretary of DHS Michael Jackson, that we develop an inter-departmental effort between DoD, DOJ and DHS to implement a LInX effort on a national scale. Secretary England believed that it was more appropriate for either DOJ or DHS to lead such an effort, but certainly offered the full support of his Department, and of his law enforcement component in NCIS. As then Chairman of the Attorney General's Advisory Committee on Information Sharing, I respectfully urged the Deputy Attorney General in a letter, co-signed by eighteen of my U.S. Attorney colleagues, to further expand LInX throughout the United States, under the auspices of each of the U.S. Attorneys who signed this letter. While the DOJ supported the efforts of the U.S. Attorney led LInX programs, it declined to take a leadership role in the further development of this vital capability.

Instead the Justice Department has taken three distinct positions that seriously compromise law enforcement information sharing in the United States. First, DOJ has retreated from its earlier standard that all legally sharable data be included in LInX or similar programs, and has substituted a far lesser standard that gives great discretion to agencies in what will be shared. Second, DOJ has refused to mandate technical and security approaches for information sharing—leaving that to local discretion and thus ensuring that only non-sensitive data will be shared with local law enforcement. And third, DOJ has chosen not to assume responsibility for leading, directing, supporting, or funding any regional information sharing system, preferring to let local interests and the market place determine the ultimate configuration of a national system. In a December, 2006 Memorandum by Deputy Attorney General McNulty, the Department of Justice withdrew from the LInX pilots and halted meaningful record sharing with state and local law enforcement. This is a tragic and harmful step backwards in local, state and federal law enforcement and cooperative counter terrorism efforts and puts our country at greater risk of terrorism attacks.

In spite of the failure of leadership at the senior level of DOJ, efforts have been made by DoD and NCIS to transition the LInX Program, which has been funded by DoD through FY'11, to the Department of Homeland Security. Former U.S. Attorney Debra Wong Yang of Los Angeles, working with Chief Bratton, Los Angeles Police Department, Sheriff Baca, Los Angeles Sheriff's Department, and Sheriff Carona, Orange County Sheriff's Department, is attempting to implement a LInX project in the Central District of California. USA Yang submitted a formal proposal for the development of this program to DOJ, and requested DOJ invest funding, and partner with DoD/NCIS to develop LInX, however, her request was denied by the DAG. The leadership of the Los Angeles law enforcement agencies subsequently petitioned DHS for funding.

I am convinced that the standards of senior executive law enforcement leadership, a cost efficient technology, and a fervent commitment to share all legally shareable law enforcement records is the recipe for successful information sharing among our 18,000 law enforcement agencies in our country. This is an effort which must be led from the most senior ranks of government, and one which must meet the operational needs of our sworn law enforcement officers and analysts who are on the front line every day attempting to find the proverbial needle in the haystack that might lead them to a terrorist support network, or to quickly capture a serial pedophile, random rapist or violent criminal. Neither crime, criminals nor terrorists know any borders. In fact, they now know how to exploit our geographical borders and bureaucratic jurisdictions to their own advantage. We need a new weapon in our fight to preserve our freedoms, and I believe we may have found such a weapon in the deployment of the LInX program.

Thank you for this opportunity to address you and this important subcommittee. I look forward to answering any questions you may have for me.

Ms. HARMAN. Chief Batiste.

STATEMENT OF JOHN R. BATISTE, CHIEF, WASHINGTON STATE PATROL

Chief Batiste. Good afternoon, Madam Chair and members of this distinguished committee.

Thank you for allowing me to be here to have this opportunity to showcase the Washington Joint Analytical Center.

In 2002 local, state, and federal law enforcement agencies in Washington joined together to develop a new system of intelligence sharing.

The key components of this system are the WAJAC, a centralized fusion center serving as a single point of intelligence collection, and the regional intelligence groups located throughout the state providing a link to a line of level personnel—to line level personnel and homeland security partners; the goal, of course, investigating crimes and preventing acts of terrorism.

The true success of the fusion center can be measured by the long-term partnership developed since the inception of the statewide integrated intelligence plan.

Situated in the same—on the same floor and in the same work area as the FBI's intelligence work group, the WAJAC employees share information real-time without the hindrance of communications barriers that have existed for decades and have only recently been breached.

For this, we can thank the tremendous efforts of the Seattle field office, the FBI, the United States attorney's office under the leadership of John McKay, and many other federal and local law enforcement leaders.

Within our fusion center, the King County sheriff's office, Bellevue police department, and the Washington state patrol detectives work hand in hand with numerous federal agencies in collection, analysis, and dissemination of intelligence information.

A prime example of the trust developed between our agencies is demonstrated in the authority established within the WAJAC by the supervision of WSP sergeant—Washington State Patrol sergeant who has the ability to assign tasks to the field intelligence personnel owned by the FBI, and the field intelligence group supervisor having the same authority to task members of the WAJAC.

In 2006 the WAJAC reviewed and disseminated over 2,000 intelligence information reports, developed 323 leads to support criminal or terrorist case investigation and provide assistance to homeland security partners on 500 separate occasions.

These numbers alone don't tell the story with regards to the exceptional work being done in this partnership.

Every day investigators and analysts from many different jurisdictions throughout this state are communicating with each other at a frequency never realized before and are sharing critical information by way of the WAJAC.

One of the primary information collection programs that has substantially served our intelligence—served our information sharing efforts is the Navy's law enforcement information exchange or the Linx system.

The WAJAC and the marine analysts use this tool on a regular basis to assist them in locating persons of interest, establishing identities, and connecting the dots on criminal investigation.

This tool has been invaluable throughout the state and has been an instrumental tool in solving a number of criminal cases.

It's imperative with regards to information sharing environment that support for Linx that we hope will continue well into the future.

Because Linx contains information only on closed criminal investigation, there still exists a need for a true intelligence database.

At present, this state does not have the necessary resources to store and electronically share critical intelligence with all agencies.

Many agencies continue to rely on e-mails, fax, and telephone conversations.

The western state information network or WSIN is one of six federally funded regional information sharing system centers.

WSIN is a force multiplied as it provides the network intelligence databases and also safety information services that law enforcement requires.

WSIN serves the five western states, including the state of Washington. I, in fact, sit on the policy board.

At our state's request, WSIN expanded its mission several years ago to include gangs and more recently all crimes including terrorism.

Washington has taken the lead in providing access to major crime units, such as homicides, burglary, and intelligence units and police agencies, but more needs to be done.

This is a proven concept and it should be fully funded rather than using federal dollars to develop additional similar intelligence systems.

Even though we've had great successes in establishing partnerships and sharing information, Madam Chair and members of this committee, we still face significant hurdles.

We need the ability to sustain these valuable programs.

Dedicated and adequate funding for WAJAC, RIGs, and WSIN is the greatest of concerns to myself and our stakeholders.

The three local law enforcement agencies and the National Guard who have assigned investigators to the WAJAC have done so on their own operational—by using their budget resources.

Additionally, all 19 contracted analysts both in the WAJAC and the RIGs are funded through the law enforcement terrorism prevention program.

In conclusion, we simply need your help.

Ms. HARMAN. Thank you, Chief. We are all here to help.

[The statement of Chief Batiste follows:]

PREPARED STATEMENT OF CHIEF JOHN R. BASISTE

Good afternoon Mr. Chairman and distinguished members of the committee. Thank you for allowing me this opportunity to showcase the Washington Joint Analytical Center (WAJAC) and our state's efforts in sharing critical criminal intelligence information.

In 2002, local, state, and federal law enforcement agencies in Washington joined together to develop a new system of intelligence sharing. The key components of this system are the WAJAC, a centralized fusion center serving as a single point of intelligence collection, and regional intelligence groups located throughout the state providing a link to line level personnel and homeland security partners. The goal: investigating crime to prevent acts of terrorism.

The true success of the fusion center can be measured by the long-term partnerships developed since the inception of the Statewide Integrated Intelligence Plan. Situated on the same floor and in the same work area as the FBI's Field Intel-

ligence Group, WAJAC employees share information real-time without the hindrance of communications barriers that have existed for decades and have only recently been breached. For this, we can thank the tremendous efforts of the Seattle Field Office of the FBI, the United States Attorney's Office and many other federal and local law enforcement leaders. Within our fusion center, King County Sheriff, Bellevue Police and WSP detectives work hand-in-hand with numerous federal agencies in the collection, analysis and dissemination of intelligence information

A prime example of the trust developed between our agencies is demonstrated by the authority of the WAJAC supervisor (a WSP Sergeant) to assign tasks to any of the FIG personnel and the FIG supervisor having the same tasking authority over WAJAC.

In 2006, WAJAC reviewed and disseminated over 2,000 Intelligence Information Reports, developed 323 leads to support criminal or terrorism case investigations and provided assistance to homeland security partners on 500 separate occasions. These numbers alone don't tell the story of the exceptional work being done through this partnership. Every day investigators and analysts from many different jurisdictions throughout the state are communicating with each other at a frequency never realized before and are sharing critical intelligence information with the WAJAC.

One of the primary information collection programs that has substantially served our intelligence sharing efforts is the Navy's Law Enforcement Information Exchange or LINX system. WAJAC and RIG analysts use this tool on a regular basis to assist them in locating persons of interest, in establishing identities and connecting the dots on criminal investigations. This tool has been invaluable throughout the state and has been instrumental in solving a number of criminal cases. It is imperative to our information sharing environment that support for LINX continues well into the future.

Because LINX contains information only on closed criminal investigations, there still exists a need for a true intelligence database. At present, this state does not have a method to store and electronically share critical intelligence with multiple agencies. We continue to relay on e-mails, fax and telephone conversations. Currently, WAJAC and other stakeholders are evaluating a statewide intelligence database to supplement our current programs. In the near future, we will be requesting Department of Homeland Security grant funding to purchase and maintain a viable database for information sharing purposes.

Even though we have had great successes in establishing partnerships and sharing information, we still face a significant hurdle in our ability to sustain this program. Dedicate funding for WAJAC and the RIGs is of the greatest concern to all stakeholders. The three local law enforcement agencies and National Guard who have assigned investigators to the WAJAC have done so out of their own operational budgets and have received no monetary compensation to backfill these talented specialists. Additionally, all nineteen contracted analysts both in the WAJAC and in the RIGs are funded through the Law Enforcement Terrorism Prevention Program Grant; funding we expect to diminish over time. Over the last three years, a significant portion of LETPP money granted to Washington State has been dedicated to funding the work completed by these contractors.

Successful programs designed to counter criminal activity and terrorism require a human element. Software programs, databases and computers alone do not fight terrorism, people do, and without the talented investigators and analysts of the WAJAC, it would be near impossible to prevent or disrupt any act of terrorism. We must have an established funding source to sustain the WAJAC into the future.

Another significant challenge we must overcome is our difficulty in staffing regional intelligence groups in all nine emergency management regions of the state. Within the rural areas of Washington, many law enforcement agencies do not have the resources available to provide full-time or in many cases even part-time investigative support for the intelligence process. Even though we have assigned grant-funded analysts to each region, without investigative support we are only meeting half of our commitment to this program. The solution to the problem may not be a simple one and with hope we will be able to further develop our RIGs to a point where they have the ability to deliver a viable service their region and the state.

When the WASPC Intelligence Subcommittee began laying the foundation for WAJAC and the Statewide Integrated Intelligence Plan they came to the same realization that no one of is as strong as all of us and no single entity can make this program work alone. We have combined our limited resources, worked collaboratively and have made a strong partnership against the terror groups who threaten the citizens of this state.

Thank you.

Ms. HARMAN. I would just—let me advise our members that each of you will have five minutes for questions, and I'll recognize myself first for five minute.

In my five minutes, let me observe that if Charlie Allen, the head of the intelligence division of the Homeland Security Department, or Michael Allen the deputy director—or Michael Chertoff, the director of the Homeland Security Department were here, I think they would have the same reaction I have, which is this is exactly how a region, a local—a state and a region should organize itself.

You have the right ideas for how the work should get done.

The problems you're having are with federal funding and connection between the federal government and you, and those are things that we need to fix, and I certainly intend to talk further to Charlie Allen and to Michael Jackson and to Michael Chertoff about this.

These are things that must be fixed, and if they won't be fixed voluntarily, they have to be fixed with legislation, as in the case of participation in the NCTC.

Let me just ask a few questions, and if you could keep your answers brief, we can ask more questions.

General Lowenberg, you mentioned the problem with prison radicalization. That is not the direct subject of this hearing, but it is directly relevant to terrorist activity.

This committee held a field hearing in Torrance, California in my district where a prison radicalized cell has been arrested and is awaiting trial.

What are the problems here and, briefly, what are you doing to make sure that you are aware of them and can prevent and disrupt them from becoming life—

General LOWENBERG. Madam Chair, I am well aware from having worked with the intelligence director from the California state prison system three weeks ago in Monterey, California, that California probably has the best assessment of the prison radicalization threat.

We have brought our state Department of Corrections into the WAJAC. Our secretary of corrections, Harold Clark, is part of the evidence group that met this last week, and so we're doing everything we can, quite frankly, to catch up with California and New York state who are frankly on the leading edge nationally in dealing with this very disturbing phenomenon.

Ms. HARMAN. Of course I don't mind that comment "catching up with California." That's good.

Chief Kerlikowske, you gave me an insight about the fact that the federal center system of information—intelligence sharing is based on a Cold War model.

When we did intelligence reform in 2004, a bill I was very involved with, that was our rant against the organization of our intelligence community.

You said it was a 1947 business model and no one can possibly operate in a 1947 business model, so we changed it.

I am very aware that there are problems with clearances at the local level and that the FBI and DHS clearances are treated differently.

Could you just give us a short bit of information on the record about the problem getting security clearances?

Chief Kerlikowske. I think one of the suggestions that was made by the major city chief's intelligence subcommittee in Charlotte was to allow, at one level, some of the background work that is now either done by federal agents or is, in fact, contracted out to retired federal agents. Why not go ahead and let some of these large local agencies do some of the basic background and preliminary work, which is so labor intensive and so time consuming?

That actually was not particularly well received by DHS.

We think it makes sense because we're trusted with protecting our communities, and we hire these officers. Why in heaven's name shouldn't we be trusted to doing the preliminary background data and information that could be helpful to getting—to moving that clearance further and faster?

Ms. HARMAN. Thank you. I think that's an excellent suggestion.

Finally for Mr. McKay and Chief Batiste. Mr. McKay, thank you for your courageous comments about the Linx system and its reception at DOJ.

Surely you know there's a rumor alive in Washington that your advocacy for that system may have cost you your job, and I know how well regarded you are. I would just like to say that if that is true, that is extremely unfortunate.

This subcommittee has looked at systems like HSNet and LEO and HSIN. I won't go into what they all are because my time is running out, but I would just like to know from both of you, do you think that Linx is a better system?

Obviously it matters—it is of critical importance how we move data and trying to get to some common system.

Do you think that Linx is the best?

Mr. MCKAY. Well, I do. I think that the elements which I've set out in my prepared remarks are important.

What's critical, Madam Chair, I think, is this: The federal government cannot command the transfer of law enforcement records to it.

I'm not sure, and I would issue a challenge to members of Congress, it's like telling a judge they can't do something, but truly trust and cooperation is required because principals of federalism would say that those 18,000 law enforcement agencies around the country cannot be ordered to transfer their records to the federal government.

What has to happen, I think what we've demonstrated in Linx, is that where we own it together—federal, state, and local—and are responsible for its administration and its security and to make sure that it's not misused and people's rights are protected, that is a cooperative governance structure that is not offered in any other system, and if there's one aspect of a system that is critically important, it is the full text records being shared, in essence, voluntarily by each participating agency because they know that if they had access to each other's data, they could make us safer.

That is the difference.

The structures exist in other places, but you will see upon analysis that they are not sharing all of their records the way we are here.

Ms. HARMAN. Thank you. My time is expired, but I want to give Chief Batiste the time to answer that question.

Chief Batiste. Madam Chair, I think I can say with confidence in support of all my colleagues across the state and region, we truly support what John is remarking with regards to the Linx system being a system that serves us well.

It does allow for independence with regards to pushing our information forward, as an agency, for viewing capabilities, yet I maintain control of that information.

Ms. HARMAN. Thank you, Chief. Thank you all.

I now recognize our ranking member Sheriff Reichert for five minutes of questions.

Mr. REICHERT. Thank you, Madam Chair.

You've all mentioned relationships, and that was key when we started to talk about Linx, and I remember when John showed up on the scene and gathered everybody together. I think everybody in this panel would agree that it was a breath of fresh air, John was, and his energy behind Linx, and the sharing of information was welcomed.

I think it brought us all together, so first of all, I would like to say, "Thank you" to John and agree with Madam Chair's comments on your courage that you show, and I appreciate all the efforts that each and every one of you put forth to make this community a safer place.

Sometimes I do miss wearing the uniform. I just thought I would share that with everybody.

Technology is the other thing that we touched on, and the Chair asked about the Linx and whether or not it's a great system.

John and I had many conversations about when the sheriff officers were going to get involved in this project, and we didn't jump until second year, and that trust had to be there.

The third thing, money.

So we have relationship, technology, money. All of these things have to come together to build a program, to build a community, to build this effort around Linx, and so now we've had the relationships are built, we've had some technology, the RAIN system here in Seattle, Linx and other systems that have come together from some of the other agencies, and granted the money has been lacking, but hopefully we'll be able to work together on acquiring more funds for this effort.

What is the status of Linx right now here in our region?

Mr. MCKAY. Linx in this region continues to operate very robustly. My understanding is that of the 150 of the something over 200 police agencies—I believe that's about right—about 200 agencies now have signed the agreements.

I believe that about 70 agencies have data flowing, and that's simply a function of having the funds to move that forward.

Of those 70, that consists of the largest agencies, including King County sheriff's office, Seattle police department, Washington state patrol, and others, so actually, in terms of data, huge amounts of data are flowing in the Linx system today.

Nationally, Linx is, I believe, up and running in five areas with seven on the boards, up to nine to include the Washington capital region and Los Angeles, and that is principally—all of that is principally being funded by the Naval criminal investigative service who should get, in my mind, a huge amount of credit here.

The technology is simple. It's not the technology.

The money is important, but it's not the money.

What is important is the agreement by agencies to actually put their data out there and share it with each other.

Frankly, it's the federal government—it's the law enforcement agencies and the federal government that need a good stick taken to them to get that done, not a carrot, a stick, and they need to put their data in there and share it, just as the Washington state patrol, the King County sheriff's office, Seattle police department are sharing all of their investigative records with the FBI and other federal agencies.

Mr. REICHERT. Another question for you, John. In this reluctance to share information, you say overclassification plays a part in that.

Is there a role that that plays?

Mr. MCKAY. I think not so much overclassification. For one thing, the Linx system is not—it's certified to the secret level, but classified data does not reside there, and mostly that would be contributed by the FBI, but, quite understood, classified data.

I think the question is whether sensitive—what agencies deem to be sensitive information is being screened out mostly by federal partners not the state and local agencies.

Chief, among these, being DEA, and, frankly, the security system that we built into Linx could take care of all of that, and I think it's a question of individual agencies relying on old days of silos and turf and saying, "Our stuff is too important to share with local police officers."

That is the wrong—that's the pre-9/11 attitude, and I can't believe that we allow it to continue to exist, and unfortunately the deputy attorney general of the United States issued a memorandum in December of 2006 going right back to that standard and letting federal agencies screen their data out of the Linx systems.

Mr. REICHERT. Thank you.

One quick question, Chief Kerlikowske. You mentioned being focused on the community, private sector.

Have you seen a difficulty reaching out to the private sector, including them in this—reluctance on their part to become involved?

Chief Kerlikowske. You know, I haven't seen any reluctance on their part because I think, as you did in King County, you have relationships established with the private sector, particularly those that contain the key infrastructure that we all know that if something happens, things are not going to work well, commerce and banking and on and on, and that's based upon the trust, but we also, of course, follow the Los Angeles art angel model and the Acam model of looking at these infrastructures and working with them, but they have to be assured that liability, and you had mentioned that earlier, is not going to attach, and they have to be assured that we are going to be as protective of that critical information on how that facility can be better protected to make sure that it is, in a proprietary way, not released.

Ms. HARMAN. The Chair now recognizes the cardinal from Washington, Mr. Dicks, for five minutes.

Mr. DICKS. Thank you Jane for bringing the hearing here.

Our same group went down to Los Angeles and saw a fusion center down there, so we're trying to get a picture of what's going on around the country, and I want to commend all of you in working together as effectively as you do in trying to overcome some of the impediments from the federal side.

Now, on this question—I think we could change this two-year limit. I mean, that's a policy matter on these analysts—funding the analysts.

I mean, if Congress stepped in and legislated and said, "The funding that we provide is available for analysts for fusion centers beyond two years," I mean, I don't see any problem doing that, and that's what you would like us to do.

Is that not right?

General LOWENBERG. The key, Congressman Dicks, is whether the grant money can be used to fund a state FTE as opposed to a contractor.

We recognize that Congress authorizes and appropriates for grant program cycles for two or three years, with each fiscal year appropriation cycle, but being told what we can expend the money for is a limitation.

As we dealt with Secretary Ridge and now Secretary Chertoff, the mantra has always been, "We would if we could, but we can't," and our question has been, "Why can't you," and it's always been, "Because OMB and the White House will not allow us to expend the money, as a matter of policy, for anything other than contract analysts or contact planners," and so we're left with these temporary hires, and frankly these information sharing centers and fusion centers then end up being a training ground, if you will, for analysts who just leave at the first opportunity to work for a federal agency where there's some relative job security, sense of stability and future employment.

Mr. DICKS. John, I want to commend you on this Linx system.

I remember we talked about this when we were having a little difficulty early on, and I think—how did the Navy wind up—the Naval criminal investigative—how did they wind up being kind of the lead on this?

Mr. MCKAY. That's a good question. It was envisioned by the FBI, and I was asked by Dale Watson, who then was the executive assistant director of the FBI, to lead the effort regionally among Washington, Oregon, and Idaho, and then the FBI disappeared after their project gateway in St. Louis crashed for different reasons, which we avoided out here in Washington state.

I went to Dave Brant, who was the NCIS director, and he agreed to run it as a pilot project in Puget Sound mainly because of the naval bases in our district, so that's how it came to be NCIS, but we felt all along that it should move away from the Department of Defense and be taken over by Homeland Security and Justice.

Mr. DICKS. I was impressed to see that Gordon England, who is a very outstanding—and who was the deputy at Homeland Security was all for this and was urging the Department of Justice and the Department of Homeland Security to go forward on this, and yet we've had all this resistance from the Department of Justice.

I just want to commend you for what you did here, and I'm glad that Linx is still operational here in the state of Washington and that you all are working together on this.

I think that's outstanding.

I think our committee ought to try to work on this to try to convince—at least maybe we can go through Homeland Security, that this ought to be a national model, which it was on the road to being until McNolty (phonetic) said, "We can't go any further" in December; is that right?

Mr. MCKAY. That's correct, and there was an important meeting between Michael Jackson, Gordon England, and Paul McNolty in which the outlines of an interdepartmental partnership, which is, I think, how this should be run, and again, as I said in my opening remarks here, you cannot find any organization in the government responsible for building the trust systems that we have here, and so if I'm sitting in your chair, I'm thinking, "Well, how is it done?"

I don't think it can be assigned alone to Homeland Security because the justice agencies have most of the federal law enforcement data through the FBI and its five agencies.

I don't think the Department of Defense should own this system for reasons that deal with civil liberties and the trust of the American people, not that we don't trust DOD, it's just that the data there is being kept on American citizens and should be overseen by civilians in the course, and I think all of us understood that when we built the system here, so the pathway to an interdepartmental partnership was there. It has not gone forward, and that's above my pay grade as to why that's happened.

Mr. DICKS. Now, I want to make sure I understand this.

Are we getting the information on people who have been convicted of federal crimes in our area?

Mr. MCKAY. Some.

Mr. DICKS. In this system.

Mr. MCKAY. Some but not all.

Mr. DICKS. They screen out some of these—you have all the local records, right.

Mr. MCKAY. You bet, Congressman Dicks.

What's happened is the local agencies are contributing all of their data into Linx essentially, not internal matters but—administrative matters, but they're investigative records, and the partnership deal that the federal government offered, and I know because I was offering it, was, and we will give you the FBI's 302s, investigative records, the DEA 6s and the federal records, which will help you solve crime in your regions and all of us to attack potential terrorism, and that promise has now been stopped by the federal government, and it is unfathomable to me why that has occurred, other than that no one is in charge.

Mr. DICKS. All right. Well, we'll go to work on it. Thank you very much. I appreciate all of your testimony.

Mr. REICHERT. Chair, allow me just one comment.

I just wanted to note that last Congress we presented a bill that—the language allowed for the full payment of analysts, and that bill is still in the hopper, so it's not a new problem, but we've also—I want to acknowledge your observation that as we've talked with members of Homeland Security and the secretary himself,

there's been a huge reluctance, as you all know, in financing local FTEs.

I think that's solely being overcome. There's a lot of work yet to do on that, and I think if we can go to rule change—some sort of a policy change route, as the General has suggested, and Norm, that would be the route to go, but we still have legislation out there too that would push—

General LOWENBERG. Congressman Reichert, if I could just respond, we very much appreciate the leadership shown in the 109th Congress, but the state's homeland security advisor has presented this issue and others to Secretary Chertoff, Secretary Jackson, and we have talked to Charlie Allen. All of that took place on April 17th in Washington DC. We still have not seen any policy shift from the agency.

Ms. HARMAN. Thank you. This was an excellent panel, and this subcommittee will follow up. These are live issues.

They are very troubling.

Our perspective, as I said in my opening remarks, is to start at the local level, find out what you need and what participation would be useful, and then view the federal government as your customer, not the other way around.

Future terrorist acts in America will, to some extent anyway, happen in our neighborhoods, and you're the folks who understand those neighborhoods, so I want to thank you for four pieces of excellent testimony.

This was a superb panel. We all learned a lot. You're excused.

Ms. HARMAN. Welcome to all of you. I will introduce you all at once, and we will start our testimony, our five-minute summaries, with Mr. Hovel, and all of you will turn the little clock around so that everybody observes the time limits.

Our first witness, Richard Hovel, is the senior aviation and homeland security advisor to the Boeing Company, a small concern that I'm also very familiar with. You have large facilities in my district in Los Angeles. Thank you for what you do.

Prior to his tenure with Boeing, Mr. Hovel served as the federal security manager for the FAA, aviation security operations division at Seatac.

Mr. Hovel began his law enforcement career with the Albuquerque police department, after which he worked for the Idaho state police as a state trooper and supervisor and criminal investigator.

Our second witness, Matt Morrison, is the executive director of the Pacific northwest economic region, PNWER, a public private partnership established in 1991 by statute in the states of Alaska, Washington, Idaho, Montana, and Oregon, and the western Canadian provinces of British Columbia, Alberta, and the Yukon territory.

For those who don't live here, this is an extremely impressive idea.

As the director of PNWER, he communicates with the state and provincial legislatures and coordinates with the working groups of PNWER in the area of homeland security.

Our third witness, Steve Stein is the northwest regional coordinator for the homeland security market sector for the Pacific Northwest national laboratory.

Mr. Stein recently completed a large project supporting the Department of Homeland Security that was focused on the assessment of the Seattle urban area's preparedness to prevent and respond to major disasters and the insertion of new technologies that would improve the region's level of preparedness.

Finally, our fourth witness, Richard Stevenson, is the president and chief operating officer for Clise Properties.

Your firm was mentioned in earlier testimony, as you know.

Mr. Stevenson has worked in the real estate and property management field for 20 years. He currently serves on the board of directors for the downtown emergency services center and the Seattle association.

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

I now ask each of you, starting with Mr. Hovel, to summarize for five minutes, and the timer will be turned on, and it it's right next to Mr. Stein.

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

Mr. HOVEL. Madam Chair, honorable members of Congress, it's very much appreciated allowing this opportunity to talk with you about this vital matter.

Since the tragic events of September 11th, 2001, and consistent with HSPD 5, the national response plan, the national infrastructure and protection plan, and the national intelligence strategy, there have been increasing strides made to integrate the private sector within the public sector information sharing framework throughout all levels of government.

As has been mentioned, in excess of 85 percent of this nation's critical infrastructure residing within the private sector, one can hardly expect the public sector law enforcement and intelligence entities to sufficiently insulate industry from risks associated with what once was primarily a criminal enterprise.

Understanding and responding to the many interdependencies between the various elements of the critical infrastructure may be more appropriately and effectively addressed by private sector ownership but with support from public sector agencies.

This is based upon a sound proactive understanding of the far reaching damage that a successful attack on critical infrastructure could have, and is somewhat contrary to the largely reactive nature of traditional law enforcement.

Because of this, information that has developed regionally may have significant impact nationally.

This was evidenced very recently by the thwarted terror plot at Fort Dix New Jersey.

To be effective in this arena, industry must have real-time access to information through fusion center capabilities in order to analyze that which may have a local or broader impact.

Conversely, federal, state, local law enforcement and intelligence entities must have access to very mature intelligence capabilities in the private sector.

The private sector has the ability to effectively acquire, interpret, analyze, and disseminate intelligence information which may originate from private sector sources.

Indeed, many companies are authorized to receive, store, and communicate classified information by employees already holding clearances.

Public/private sharing of intelligence information, as we've all said, is a function of trust, and as we well know, all trust is local, which provides the very foundation of the fusion center concept.

Capitalizing on the already significant relationships that exist between the public and private sectors here in the northwest and to mitigate the ever-changing risk, Boeing is in the process of assigning an analyst to the Seattle FBI fusion center.

Fortunately the government has put in place a mechanism which enables private industry to enter into such collaboration, namely the Federal Safety Act.

Boeing is currently working with the Department of Homeland Security in an effort to submit an application for protection under that act.

Hopefully this will be the first of many, many similar efforts across the nation that will establish a collaborative partnership between public sector and industry and protect our critical infrastructure more effectively and expeditiously.

A communication hub, around which the fusion concept could be built would use the collaborative efforts of both the private and public sectors, working in conjunction with the Pacific Northwest economic region center for regional disaster resilience have formed the community-focused northwest warning and response network, otherwise known as NWWARN.

While the genesis of this was based upon the emergency response network model implemented in the southwest, NWWARN is a much more robust, all hazards, all threats communication tool.

This network provides multidirectional communications between the FBI and both public and private interests across the five northwestern-most states of Alaska, Montana, Idaho, Washington, and Oregon.

Additionally, we are in formative stages of establishing a virtual regional information fusion center pilot project.

It would provide two-way information sharing on a multilayered, secure, and very resilient system with analysis produced by a team of core resident, local, and state experts with virtual analysts from different sectors and disciplines.

It would be using a largely virtual database to enable integration, assessment, and secure tailored dissemination of information provided to key stakeholders.

The analysis would be used for organizational and collective decision making in crafting public information.

The virtual capability will interconnect state, local, private sector, now defense, and other stakeholder capabilities while avoiding duplication of effort, proliferation of analytical products, and competition for hard-to-find analytical staff resources.

VerDate Nov 24 2008 07:58 Jul 07, 2009 Jkt 000000 PO 00000 Frm 00038 Fmt 6633 Sfmt 6601 H:\DOCS\110-HRGS\110-42\48917.TXT HSEC PsN: DIANE

It will be—it will enable federal authorities to have a single focal point to efficiently and securely provide intelligence and other sensitive information to a wide range of customers.

This pilot would provide a model which could be customized by states and localities across the nation.

The overarching purpose of these collective efforts is to better identify infrastructure interdependencies and preparedness gaps.

They focus emphasis on identifying asset criticality, managing disasters, and furthering the trust factor between key stakeholders while moving law enforcement and intelligence communities beyond the "need to share" philosophy toward a "responsibility to provide" model.

I thank you very much for the opportunity again, for the time and effort and the support you all are providing in this hearing.

Ms. HARMAN. Thank you, Mr. Hovel.

[The statement of Mr. Hovel follows:]

PREPARED STATEMENT OF RICHARD E. HOVEL

Since the tragic events of September 11, 2001, and consistent with **HSPD–5,** the **National Response Plan, National Infrastructure Protection Plan** and the **National Intelligence Strategy,** there have been increasing strides made to integrate the private sector within the public sector information sharing framework throughout all levels of government.

With approximately 87 percent of this nation's critical infrastructure residing within the private sector, one can hardly expect public sector law enforcement and intelligence entities to sufficiently insulate industry from risk associated with what was once [primarily] "criminal enterprise". Understanding and responding to the many *inter-dependencies* between the various elements of the critical infrastructure may be more appropriately and effectively addressed by private sector ownership, with support from public sector agencies. This is based upon a sound *pro-active* understanding of the far-reaching damage that a successful attack on critical infrastructure could have—and is somewhat contrary to the largely reactive nature of traditional law enforcement.

Because of this, information that is developed regionally may have significant impact nationally. This was evidenced by the recently thwarted terror plot at Fort Dix. To be effective in this arena, industry must have real-time access to information through Fusion Center capabilities, in order to analyze that which may have a local or broader impact. Conversely, federal, state and local government, law enforcement and intelligence entities must have access to mature intelligence capabilities in the private sector.

The private sector has the ability to effectively acquire, interpret, analyze and disseminate intelligence information—which may originate from private sector sources. In deed, many companies are authorized to receive, store and communicate classified information by employees already holding clearances. Public/private sharing of intelligence information is a function of "*trust*" and as we well know, "all trust is local" which provides the very foundation for the Fusion Center concept.

Capitalizing on the already significant relationships that exist between the public and private sectors in the Northwest and to mitigate ever-changing risk, Boeing is in the process of assigning an analyst to the Seattle FBI Fusion Center. Fortunately, the federal government has put in place a mechanism which enables private industry to enter into such collaboration, namely, the federal SAFETY Act ("Support Anti-terrorism by Fostering Effective Technologies Act of 2002.") Boeing is currently working with the Department of Homeland Security in an effort to submit an application for protection under the SAFETY Act. Hopefully, this will be the first of many similar efforts across the nation that will establish a collaborative partnership between the public sector and industry, and protect our critical infrastructure more effectively and expeditiously.

A communication hub, around which the fusion concept could be built would use the collaborative efforts of both the private and public sectors, working in conjunction with the Pacific NW Economic Region (PNWER) Center for Regional Disaster Resilience have formed the community-focused Northwest Warning and Response Network (NW WARN). While the genesis of this was based upon the Emergency Response Network (ERN) model implemented in the Southwest, NW WARN is a much

more robust "all hazards—all threats" communication tool. This network provides multi-directional communications between the FBI and both public and private interests across the five Northwestern-most States of Alaska, Montana, Idaho, Washington and Oregon.

Additionally, we are in the formative stages of establishing a virtual Regional Information Fusion Center Pilot Project (RIFCPP) that would provide two-way information sharing based on a multi-layered secure and resilient system with analysis produced by a team of core resident local and state experts with virtual analysts from different sectors and disciplines. They would be using a largely virtual database to enable integration, assessment, and secure, tailored dissemination of information provided to key stakeholders.

This analysis would be used for organizational and collective decision-making and crafting public information. This virtual capability will interconnect state, local, private sector, defense and other stakeholder capabilities while avoiding duplication of effort, proliferation of analytical products, and competition for hard-to-find analytical staff resources. It will also enable federal authorities to have a single focal point to efficiently and securely provide intelligence and other sensitive information to a wide range of customers. This pilot would provide a model which could be customized by states and localities across the nation.

The overarching purpose of these collective efforts is to better identify infrastructure interdependencies and preparedness gaps. They focus emphasis on identifying asset criticality, managing disasters and furthering the "trust-factor" between key stakeholders while moving the law enforcement and intelligence communities beyond the **"need to share"** philosophy toward a **"responsibility to provide"** model.

Thank you for your time and support in finding solutions to take advantage of both public and private sector capabilities.

Ms. HARMAN. Mr. Morrison.

STATEMENT OF MATT MORRISON, EXECUTIVE DIRECTOR, PACIFIC NORTHWEST ECONOMIC REGION

Mr. MORRISON. Thank you, Madam Chair.

I'm very happy to be here.

I think the title of this hearing is—exactly cuts to the centerpiece of what we need in this country in order to be better prepared for both manmade and natural hazards.

I would say that our work has been largely with the critical infrastructures and trying to understand regional disaster resilience, and the information sharing piece is a vital cornerstone of regional resilience.

As yet, my experience at DHS has not focused in any meaningful way on cross sector challenges to the all-important task of building regional resilience.

We have sector stove-pipes in all of our information sharing.

What I call the resilience tautology is: Resilient assets and infrastructures require resilient regions; resiliency requires understanding which assets are critical in any specific scenario; understanding criticality depends upon understanding the interdependencies between and among our critical infrastructures; interdependencies remain undiscovered in stove-piped sector specific planning; and understanding interdependencies require cross sector information sharing; and cross sector and public/private information sharing requires creation of an environment of trust where stakeholders feel safe to share their vulnerabilities with each and other and with first responders and government.

Comprehensive planning for resiliency cannot be done without having all the key stakeholders together sharing in a trusted environment.

That's what we're missing.

This process cannot be done by government or the private sector alone but only in a trusted partnership.

So our work—I mean, it's been amazing.

The HSIN you mentioned. You know, we—before there was a Homeland Security Department we met with the office—the White House Office of Homeland Security.

They came out and endorsed that we could be a pilot at HSIN CI, it was called.

We built 200 vetted professionals throughout the private sector, throughout the region. They promised us many times that Canada could be a part of it, but that never happened, but last month they just wrote a letter to everyone and said, "Sorry. We're closing it down."

This was shocking to me.

I mean, when really it's—the real asset here is trust, and you build that with stakeholders, key stakeholders, so it's been an unbelievable experience in trying to just develop an opportunity for us to share critical information between the silos, and here we have a real great test bed.

I mean, the—we get it out here. We've really done the work. We've had all these exercises. We've looked at earthquakes to cyber terrorism to pandemic flu and had all 17 infrastructure sectors from the whole region working together.

It's wonderful, and what we lack is this—there's such a control—DHS just wants to control everything, and they wouldn't let us share with each other, which is really the ultimate goal of having resilience, and it's not a technology issue.

I think it was mentioned very nicely on the first panel that we can do this if we'll just be allowed to do it, and so of course since they shut down what we were working on with NWWARN, we still have the board and all the people, and we're building a local model, but it would behoove the government to be listening to the traffic between the utilities and the water systems and law enforcement because we all need to know this information, so we set up a thing with gatekeepers and—you know, we've worked out the requirements for the last four years.

I guess I want to say that I do think it is the responsibility of the federal government to find a way to incentivise and fund and to—the startup and technical support to develop regional public/private partnerships in communities and states addressing regional resiliency, public/private information sharing, and critical infrastructure security.

I think this could be done by a competitive programming providing even as little as $250,000 seed money for interested states and regions to develop something like what we've done here, which is so doable.

I would like to suggest that you use this region as a test bed to work with regional stakeholders to develop solutions for critical challenges that we all face.

I'm happy to say that with the support of the committee, there has been support from the department of the Navy, from DTRA, the defense threat reduction agency—is working on a project here because of the stakeholder collaboration, and I think that there's great opportunities.

I would say that federal support for technical assistance and encouragement is essential to spearhead, develop, and initially sustain cross sector collaboration to identify needs and cost effective solutions, activities and pilot projects to meet homeland security and disaster resilience challenge.

The area of information sharing is absolutely vital to move forward with the support for developing a regional information fusion center that incorporates these critical infrastructure private sector opportunities, both analytical capabilities, that we see it as a virtual center that would allow this kind of communication.

In my formal remarks there is a more detailed explanation of a pilot that we feel could be a great model for the nation.

Ms. HARMAN. Thank you very much, Mr. Morrison.

[The statement of Mr. Morrison follows:]

PREPARED STATEMENT OF MATT MORRISON

Mr. Chairman and Members of the Committee,

I commend you for the title of today's Seattle Field Hearing: "Building a Partnership Strategy: Improving Information Sharing with State & Local Law Enforcement and the Private Sector".

This is exactly the right topic to be addressing as it cuts to the centerpiece of how this nation needs to be and can be better prepared to face the wide range of natural and man-made hazards with a comprehensive system of systems approach to preparedness and the mitigation of vulnerabilities in our communities.

Since 9–11 there has been a great deal of focus on physical protection, and infrastructure sector specific plans. As we all saw this week, Secretary Chertoff announced the Sector Reports under the National Infrastructure Protection Plan have finally been released.

While it has been a positive step to increase the security of our infrastructures to terrorist attacks, as we saw with Hurricane Katrina, there is a pressing need to focus on cross-sector cooperation, coordination and information sharing to achieve regional disaster resilience. As yet, DHS has not focused in any meaningful way on cross-sector challenges to the all- important task of building regional resilience. Infrastructures and essential service providers in a region are tightly interdependent and subject to cascading failures that can incapacitate entire communities. What this means is that a utility or other service provider may have the best security possible and still have its operations or business practices damaged or disrupted.

Resilient regions are able to bounce back from any kind of disaster with limited impacts on public health and safety, the economy, and national security. If we want to have 'Resilience' from either a natural hazards or a terrorist attack we must be able to understand the vulnerabilities caused by regional interdependencies, what assets and facilities are truly critical, and determine cost-effective ways based on risk to prevent or mitigate these vulnerabilities. The only way to gain this understanding is through cross-sector partnerships that foster local trust among all the key stakeholders that have roles or vested interests in providing critical products and services or which have emergency preparedness and management responsibilities. This is a large number of organizations—all levels of government, private sector, non-profits, academic and research organizations and community institutions.

What I have just described is what we call the 'Resilience Tautology'. To state it simply,

- Resilient assets and infrastructures require resilient regions
- Resiliency requires understanding which assets are critical in any specific scenario
- Understanding criticality depends upon understanding the interdependencies between and among critical infrastructures (85% of which are privately owned). Criticality is dynamic and changes during an incident, often in unanticipated ways
- Interdependencies remain undiscovered in stove-piped sector specific planning
- Understanding interdependencies require cross sector information sharing

- Cross sector and public/private information sharing requires the creation of an environment of trust where stakeholders feel 'safe' to share their vulnerabilities with each other and with first responders and government

To emphasize, comprehensive planning for resiliency cannot be done without having all the key stakeholders together—sharing in a trusted environment—which provides a value added resource to each and all of them. Regional Resilience requires that procedures and protocols for information sharing be worked out in advance of any incident, and that stakeholders work together to mitigate vulnerabilities and address shortfalls in a consistent framework within a public private partnership. This process cannot be done by the government or the private sector alone, but only in a trusted partnership with all key stakeholders in a community.

PNWER's Long Role in Fostering Regional Infrastructure Security and Disaster Resilience

PNWER has been working since the September 1, 2001 attacks to develop ways and avenues for information sharing among the public and private sectors and other stakeholders through outreach, developing and conducting workshops, exercises, interdependency forums, pilot projects and leading/facilitating Partnership activities, including regular meetings.

PNWER is unique in that it has a statutory mandate from five states: Alaska, Washington, Idaho, Oregon, and Montana, as well as the western Canadian provinces of British Columbia, Alberta, and the Yukon. PNWER's board is made up of elected state and provincial legislators, the Governors and Premiers of all jurisdictions, and Industry leaders in the major industries in the bi-national region. Our focus is the economy of the region, and the safety and quality of life for all citizens. After September 11, our governing board was very concerned about the safety of our communities, as well as safeguarding against the potential threats to our economy. In consultation with all Governors and Premiers, it was agreed that the one area that was not being fully addressed was the interface between private infrastructures and government. It was this gap that PNWER's Center for Disaster Resilience was launched to address.

Throughout the winter of 2002, the Pacific Northwest Partnership for Regional Infrastructure Security created by PNWER began preparation for the first multi-sector, multi-jurisdiction, cross border exercise focused on critical infrastructure interdependencies called Blue Cascades. This unprecedented exercise was the first in a series and was held outside of Portland, OR in June 2002 and was attended by more than 200 representatives from all eight jurisdictions in the PNWER region. The exercise was based on a terrorist attack on some of the Bonneville Power Administration's important assets, bringing down much of the northwest power grid for weeks to months. The exercise focused on cascading impacts involving all critical infrastructure sectors, as well as law enforcement. It was eye-opening to all participants

After Blue Cascades I, We continued to have quarterly meetings of the Partnership, and held an Action Planning meeting to address shortfalls identified in the exercise. This process led to a regional Action Plan comprised of a number of recommended initiatives, some of which have been accomplished and some which are ongoing. The most notable finding from the exercise was the high priority all stakeholders placed on the need for a regional information sharing mechanism for all key stakeholders. We took this identified need to the then Whitehouse Office of Homeland Security—CIO Steve Cooper, and Col. Bob Stephan. In the spring of 2003 we hosted a meeting with the Seattle FBI to establish a pilot for the northwest which became the NorthWest Warning, Alert, and Response Network (NW WARN.GOV).

NW WARN developed a public—private board of key stakeholders, and a gatekeeper community of over 100 key leaders in all 17 infrastructures. We petitioned to become a pilot project in a new program DHS was launching based on the Dallas, TX Emergency Response Network (ERN), which was a largely law enforcement-focused model out of the Dallas FBI. After much delay, DHS agreed to let us be part of the new pilot, which became known as HSIN-Critical Infrastructure or HSIN–CI.

Over the past four years, we have worked to build the membership of this information sharing system to over 2,000 vetted key stakeholders in our region. We developed a handbook, detailed requirements for information sharing among sectors, but never received the support we needed from DHS for implementation. Instead, Last month, DHS discontinued the program and sent a letter to all 2000 professionals to announce the cancellation. Our NW WARN Board nonetheless has continued to meet, and we are determined to build the functionality into the system that we have always wanted to be able to share critical information among sectors and with law enforcement and emergency management.

Blue Cascades II—focus on Cyber Systems

Key stakeholders elected to develop a second regional interdependencies exercise with PNWER's help the following year. Blue Cascades II was again a grassroots effort to address an issue that the first exercise had left out—cyber vulnerabilities and the gap between physical and cyber preparedness. A Scenario Design Team, made up of over 30 organizations, labored over six months developing the scenario, which brought out the importance of cyber systems and information security.

The process of bringing private sector key individuals, who live and breathe the vulnerabilities of their systems, together with law enforcement and emergency management was incredible. ,e had every participant sign a non-disclosure agreement to participate in the exercise. For many first responders, it was the first time they realized just how the communications systems they relied upon could be compromised by a cyber attack that could leave them essentially 'in the dark' and unable to communicate.

The exercise led our state Homeland Security Director to state that were it not for the exercise, he would not have known about what he considered one of the top five vulnerabilities in the state—pointing out that both DOD and DHS had missed listing this particular issue on their state-wide assessment, but was brought out by the process of stakeholder information sharing during the exercise.

Blue Cascades III—focus on Earthquake Preparedness

Following Katrina, stakeholders met to discuss what was the Northwest's 'Katrina'. All agreed that it was the 9 point subduction zone earthquake that is anticipated to hit off the coast from British Columbia to California sometime in the next 50 years or so. (The last one was on Jan. 26, 1700, and records show that it has happened on average every 300 years). This exercise was led again by PNWER with critical infrastructure stakeholders who wanted to address the long term recovery and reconstitution issues after an extreme disaster. It was a two day exercise involving over 350 participants.

Lessons Learned for Information Sharing. While previous Blue Cascades exercises demonstrated the need for interoperable communications, in BLUE CASCADES III at issue was the impact of the loss of telecommunications and critical IT systems and how these systems and particular emergency communications could be made more resilient (able to withstand a subduction zone quake and expeditiously recover with minimal damage). Some participants pointed to mitigation measures, including building more systems redundancy and developing alternative, mobile, and easily deployable wireless-based communications. There was need for "situational awareness"—knowledge of what was happening throughout the region—as the disaster unfolded, to enable optimal decision-making on response (e.g., dispatching personnel and other resources where needed, prioritizing service restoration, determining evacuations routes and sheltering locations, etc.). Private sector and other non-government organizations emphasized the need for their inclusion in regional preparedness planning, not just with the state or provinces, but with municipalities. One water systems representative stated that he would like to hear from government less of "I got you covered—don't worry" and have more cooperation. An energy official noted that "cooperation is a two-way street and public and private sector representatives must be willing to meet and participate in the many infrastructure and planning initiatives currently underway, and not just at the exercises that come along every now and again." A telecommunications representative reflected sentiments of other participants that companies are reluctant to share information directly with government. Through participating in "lots of exercises", however, they can determine what information they need and what needs to be shared. As one participant put it, "Trust relationships are paramount in creating an environment where it is felt that information can be shared safely, and in confidence." A power company official cited the need to know what the critical loads are for the other sectors and that without this knowledge it would be difficult to establish restoration priorities. Non-electric sectors wanted to learn more about how power is capable of being restored and work with utilities to make modifications to their systems so restoration of power to critical infrastructure can be accomplished quicker.

The Blue Cascades III scenario of an earthquake—an unexpected act of nature—precluded the need for participants to address alert and warning in the Puget Sound Region through NWWARN. A major issue, however, was the tsunami warning system. Participants questioned whether the many thousands of individuals along the coast from British Columbia to San Francisco would have ample warning time to reach higher ground, or even receive a warning given the widespread regional power outage and telecommunications failures generated by the earthquake. On response or recovery/restoration issues, it was unclear in the exercise how decisions would be made on trade-offs that needed to be made within a short time frame. An example was the issue of whether to use scarce water for putting out the fires from gas leaks

and pipe ruptures or to save it for human consumption. Moreover, organizations had no way to gain information on what resources were available. For example, Cingular noted that it has "loaner" cell phones, portable cell phone sites, and cellular phones that plug into laptop computers to create internet connectivity. The federal government was said to be working on a process to channel private sector assistance to government authorities in a crisis.

There was much discussion in Blue Cascades III on priorities regarding service restoration in an environment when there would be great demand and competition for being towards the top of the prioritization list. Some participants pointed out that states, localities, and utilities had already established priority lists, and these should be followed. Other participants, such as the Postal Service, expressed concern that they were far down on the list and would not gain services for "some period of time". Still others noted that priority restoration should be flexible depending on need. At the same time, most participants appeared to understand that in a major disaster priority lists would likely "go out the window", and that infrastructure interdependencies should play a role in which services were restored and in what sequence. As one participant put it, "priorities are different depending upon where you sit." In addition, there was also some discussion related to what is most critical. Participants questioned whether is it the water supply system, hospital, transportation, food and agriculture operation, or life safety such as emergency services. As an electric power representative observed, "understanding what "critical load" is will help establish restoration priorities."

Blue Cascades IV—Pandemic Preparedness and Critical Infrastructures

Blue Cascade IV held in January of this year focused on impacts on critical infrastructures and essential service providers from a Pandemic Influenza attack. We included the excellent experience of the Ontario Emergency Management director who had handled the SARS epidemic in Canada, and looked again at the interdependencies of our critical infrastructures and how there might be cascading impacts due to workforce shortages. It was evident that more needs to be communicated to private sector critical infrastructures, and that HHS and DHS need to be better coordinated for incident management in a Pandemic.

We were fortunate to have the HHS Director of Critical Infrastructure Protection, Dr. Tom Sizemore for a planning session for the exercise and have the Regional Director for HHS participate in the event..

Again, it was clear that information sharing among critical infrastructures, government, and public health agencies was absolutely vital, and not being well addressed. Our region has some of the leading private sector businesses who have done landmark work in Pandemic preparedness and were willing to share their efforts with their peers. Boeing, Microsoft, Washington Mutual, Puget Sound Energy, Starbucks, Bonneville Power Administration are some of the leading companies in this area in the world. We are in the process of developing an Action Plan based on the lessons learned from the most recent exercises that can become part of a regional pandemic preparedness strategy.

Recommendations:

The following are based on PNWER's long experience of working with stakeholders to develop and implement regional disaster preparedness initiatives.

The Federal Government should fund the start up and provide technical support to develop regional public/private partnerships in communities and states addressing regional resiliency, public/private information sharing, and critical infrastructure security. This could be done by a competitive program providing up to $250K to allow seed money for interested states and regions to move forward and develop an ongoing process to build trust and develop awareness among key stakeholders of public and private infrastructures on vulnerabilities and mitigation measures associated with regional interdependencies.

The eight jurisdiction PNWER region is demonstrably ahead of the nation in building cross-sector trust among regional stakeholders to foster disaster resilience. DHS, the Department of Defense, and other federal agencies can use the PNWER region as a test-bed to work with regional stakeholders to develop solutions for the critical challenges that face the nation today—including developing a model regional public/private sector, all-hazards information fusion center and the protocols and procedures to allow virtual information sharing among all critical infrastructures, law enforcement, emergency management, and other key stakeholders. PNWER commends certain federal agencies, DHS/ Science and Technology Directorate, the Defense Threat Reduction Agency, and the U.S. Department of Energy for willingness to provide modest support for a few significant projects focusing on inter-

dependencies challenges. Much more of this type of support needs to be provided to undertake many of the recommended solutions to preparedness shortfalls identified in the respective Blue Cascades exercises that are enumerated into the Blue Cascades Integrated Action Plan.

Summary

To summarize, in addressing disaster resilience, our focus must be not just inside organizations or on sectors but outside the fence, cross-sector, grass roots to national level, focus on all threats (including aging and deteriorating infrastructures), and all-hazards and regional in scope. We must reminder always that all disasters are local and that all trust is local.

We have to also keep in mind the "Resilience Tautology"—that resilient assets and infrastructures require resilient regions; regional resilience requires an understanding of infrastructure interdependencies and associated vulnerabilities, consequences of disruptions under specific scenarios, and risk-based mitigation; and that regional risk assessment and management requires collaboration and information-sharing among key stakeholders, which includes regional DOD assets.

Lastly, federal support—funds and technical assistance and encouragement—is essential to spearhead, develop, and initially sustain cross-sector collaboration to identify needs and cost-effective solutions—activities and pilot projects—to meet homeland security and disaster resilience challenges. In the area of information sharing, it is important to move forward with support for developing a regional information fusion center that incorporates the private sector that can be a model for the nation. Following is a description of this essential pilot project for which PNWER has been tasked to set up and facilitate a Task Force to develop.

Attachment 1

Northwest Warning, Alert and Response Network

2007
NWWARN Regional Governnance Board*

Gennie Thomspon
NWARN President

Brandon Hardenbrook
Pacific Northwest Economic Region; NWWARN Vice President

Hal Cchlomann
Washington Association of Sewer and Water Districts; NWWARN Secretary

Marty Prewett
FBI, Seattle
NWWARN Regional Manager

Joe Huden
City of Everett

Mary Robinson,
Puget Sound Energy

Director
King County OEM

Bryant Harrison
FEMA Region X

Dick Hoval
Boeing

Bill Cooper
Microsoft

Scott Heinz
WA Military Department

Kevin Zeller
WA State Patrol

Rod Hilden
Port of Seattle

Paul Schieck
Seattle Mariners

Paul McIntyre
Alerwood Sewer & Water

** Partial List*

TO: MAJOR GENERAL LOWENBERG, WA ADJUTANT GENERAL
FROM: NWWARN REGIONAL GOVERNANCE BOARD
1SUBJECT: NORTHWEST WARNING, ALERT AND RESPONSE NETWORK
DATE: MAY 15, 2007

Dear General Lowenberg,

Our officers wanted to update you on all the changes occurring with NWWARN and appreciate the continued interest and support of you and your staff. These changes have been very challenging and will ultimately all be very beneficial.

NWWARN was designed and developed locally about five years ago with the assistance of the FBI, Pacific Northwest Economic Region (PNWER), and regional private/public critical infrastructure leaders. Along with similar information sharing networks in other geographic regions, we all became the pilot for DHS' goal of creating a national private/public information sharing network. We were collectively known as the Homeland Security Information Network—Critical Infrastructure (HSIN–CI).

This DHS goal was met in 2006 and a GAO analysis of all the DHS HSIN programs stated that HSIN–CI was the only successful program due in large part to its extensive membership of local decision makers across all private and public critical infrastructures. However, DHS then switched to a new technology source that could not support the system. This resulted in the loss of our national and regional websites.

We understand the need to be regionally owned, controlled and managed to ensure our continued existence and to better address our region's issues and needs, such as the 2010 Olympics security, PNWER and the Pacific Northwest Emergency Management Agreement (PNEMA). We will be independent but continue our close relationships with L/S/F government agencies, jurisdictions, and all private and public infrastructures.

Our challenge has been to select a new technology vendor to rebuild our system/network, and to obtain initial and ongoing funding. This is underway and we expect to have our website restored within 90 days, followed by acceptance of new members and full restoration of our services.

The benefits to all of us will be our incorporating new features and functions, and expanding our membership to include all of our interdependent NW states and provinces. These will be Alaska, Idaho, Oregon, Montana, and Washington, plus Alberta, British Columbia and the Yukon.

In closing General, we again want to thank you for your support, the support of your staff, and the support of the Washington State Military Department and Emergency Management Division. We have worked closely with the Washington State Committee on Homeland Security's Critical Infrastructure Protection Subcommittee and recognize that NWWARN is important to the success of protecting our state's critical infrastructure. We have proven our worth to the state and region, and once we have our funding issues settled, we will be able to solidify our standing and expand.

Respectfully,

Gennie Thompson,
NWWARN President

Attachment 2

Pacific NorthWest

Economic Region

Pacific Northwest Center for Regional Disaster Resilience

The Pacific Northwest Center for Regional Disaster Resilience (RDR Center) serves public and private sector organizations and other key stakeholders to identify

preparedness gaps and implement cost-effective prevention and mitigation measures to address them. The RDR Center is an integral element of the Pacific NorthWest Economic Region (PNWER), a statutory, public/private partnership chartered in 1991 by the Northwest states of Alaska, Idaho, Montana, Oregon and Washington and the Western Canadian provinces of British Columbia, Alberta, and the Yukon Territory. As the implementation manager of PNWER's Homeland Security Program, the RDR Center's mission is to improve the ability of the Pacific Northwest to protect its critical infrastructures and to withstand and recover from all-hazards disasters. The RDR Center does this through raising awareness of infrastructure interdependencies, providing training and education, and developing tools, technologies, and approaches that build on existing capabilities and can be utilized across the United States, Canada, and the international community.

Building on Five years of Progress

The RDR Center's mission is continuing and building upon a long legacy of PNWER's work with states, municipalities, and other regions to secure interdependent infrastructures and develop disaster resilience. The first initiative to address regional infrastructure security issues was the creation of The Partnership for Regional Infrastructure Security in November, 2001. The Partnership brought key private stakeholders representing the critical infrastructures in the eight-jurisdiction PNWER region together with the federal, state and provincial officials responsible for emergency management and public safety. These stakeholders, along with elected officials from each state and province, identified opportunities for acting proactively to strengthen their infrastructures.

Since then PNWER has organized with the regional stakeholders three critical infrastructure interdependencies exercises over the past four years and is now developing a fourth (the Blue Cascades Series). Each exercise has been designed by the stakeholders, reflected regional concerns, and produced an Action Plan of projects and activities to address lessons learned. Blue Cascades I, held in Portland, Oregon in June 2002, was conducted under the auspices of the newly created Pacific Northwest Partnership for Regional Infrastructure Security and sponsored by the U.S. Department of the Navy's Critical Infrastructure Protection Office, FEMA Region 10, and the Canadian federal government. The exercise centered on raising awareness of interconnections among the region's critical infrastructures and resulting vulnerabilities associated with largely physical attacks and disruptions. Blue Cascades II, held in Seattle in September 2004, was sponsored by King County, the U.S. Department of Homeland Security's National Cyber Security Division, Puget Sound Energy, Microsoft, and TransCanada. Blue Cascades II centered on cyber events to meet stakeholder needs to learn more about cyber threats, disruptions, and impacts. Blue Cascades III, held in Bellevue in March 2006, was supported by the U.S. Department of Homeland Security, Navy Region NW, King County, Microsoft, CH^{2}M HILL, Cingular Wireless, Puget Sound Energy, BPA and CTC. Blue Cascades III focused on the response, recovery and restoration after a M9 subduction zone earthquake. Blue Cascades IV, which focuses on the impact of infrastructure interdependencies on pandemic preparedness, is now under development and scheduled in January, 2007.

As a result of these regional initiatives, PNWER has undertaken pilot projects with DHS, the Department of Energy and other federal entities, including development of a regional alert and warning system (NW WARN), a regional energy vulnerability assessment, and an interdependencies identification tool for stakeholder use.

RDR Center Today

The RDR Center is building on this extensive foundation of activities through:

- Creating and fostering cross-sector partnerships focused on infrastructure security and disaster resilience;
- Developing and conducting regional infrastructure interdependencies initiatives focused on various threat scenarios that include regional cross-sector/cross discipline workshops and exercises to better understand threats, vulnerabilities, and develop strategies for action to address them;
- Developing requirements for stakeholder-validated projects and activities to address readiness gaps and improve regional resilience;
- Seeking funding and other resources to support regional pilot projects and other activities and to enable state and local agencies to address regional preparedness needs;
- Overseeing the implementation of priority projects and activities in a cost-effective, timely and ethical manner;
- Conducting outreach and develop and facilitate seminars, workshops, and targeted exercises to raise awareness and test the level of preparedness.

- Communicating stakeholder validated regional disaster resilience recommendations to state and provincial governments and policymakers
- Providing information through a dedicated web portal www.pnwer.org/portal/ and other mechanisms about resources on CIP and regional disaster resilience issues, lessons learned, best practices; and on upcoming homeland security, emergency preparedness, and related events. Tools include:
  - A Document Library that can be searched by infrastructure sector, hazard, threat, and jurisdiction;
  - An Events Calendar with dates and information on conferences, exercises, and other events concerning disaster resilience and critical infrastructure protection;
  - A Stakeholders Forum which allows registered users to interact with each other and with a panel of knowledgeable stakeholder representatives.

Lastly, through its **Consortium** of multi-disciplinary experts from recognized research institutions and technical assistance providers, the RDR Center provides a **Center of Excellence** with access to expertise, best practices, and lessons learned from CIP and preparedness conferences, workshops, exercises, in addition to other useful resources.

RDR Center Structure

As the program implementation focal point for homeland security and disaster resilience for the multi-jurisdiction Pacific NorthWest Economic Region, the RDR Center is a non-profit, public-private collaborative organization.

Board of Directors. The RDR Center Board of Directors, comprised of state and provincial legislators and distinguished independent experts, provides strategic direction and general oversight the Center's activities.

RDR Center Director and Administrative Staff. The Director handles operational activities of the Center and ensures effective program execution and quality control. The Director determines with PNWER staff budgetary /resource requirements and seeks means to fulfill these requirements.

Regional Steering Group. The Steering Group is comprised of the chairs of regional and state partnerships/collaborative mechanisms within the PNWER eight member jurisdictions. The Steering Group prioritizes and determines what activities will be included in the RDR Center's programmatic activities, reviews progress on projects, and provides recommendations.

Project Requirements and Oversight Work Groups. Cross-sector, multi-disciplinary Work Groups of stakeholder organizations representing interested regions are responsible for developing requirements for individual projects and monitoring project implementation.

State/Provincial Council. A Council of state and provincial senior officials charged with homeland security and disaster resilience provides guidance to the Steering Group and the RDR Center Director on the types of projects that should be undertaken to build upon and improve existing capabilities.

Federal Advisory Group. Comprised of U.S. and Canadian federal agencies with homeland security, public safety and emergency management responsibilities, the Advisory Group provides advice and as appropriate, technical and policy assistance on program implementation challenges that have national implications.

RDR Center Technical Assistance Consortium. The Consortium is comprised of research and technical service provider organizations that have expertise in the broad range of Critical Infrastructure Protection and disaster resilience needs (national laboratories, academic research institutions, contractors/consulting firms). Members of the Consortium, based on their capabilities, team to assist state and local stakeholders to develop requirements for specific projects and activities and provide the technical expertise necessary for program implementation.

RDR Center Sources of Support

Overall support for the RDR Center comes from PNWER member State and Provincial dues (which are set by statute), private sector partnership members, as well as government programmatic funds and grants; foundations, and other contributions.

Attachment 3

REGIONAL INFORMATION FUSION CENTER

PILOT PROJECT

Purpose

The following paper outlines what is required to build on existing capabilities for cross-jurisdiction/public-private collaboration and information-sharing to develop a **state-wide, holistic regional information sharing and analysis capability** to meet the following broad security and disaster resilience needs:

1. Collection, integration, analysis, and dissemination of all-source threat-related information for law enforcement and infrastructure protection;
2. Understanding regional interdependencies and determining critical infrastructure/key resources (CI/KR) vulnerabilities and risk;
3. Disaster/incident preparedness and management.

The pilot project would encompass and leverage various activities supported by components of the U.S. Department of Homeland Security that currently are underway to improve regional information sharing and analysis capabilities, including the Washington Joint Analytic Center (WAJAC)) and the developing Seattle/King County fusion center; NWWARN, and the Puget Sound Partnership Interdependencies template project. The pilot project would also leverage systems and procedures for information sharing already developed by DHS, DOD and other entities.

The end-result would be a state-wide "virtual" Regional Information Fusion Center (information sharing and analysis capability) with protocols/procedures that can cost-effectively provide public, private and other key stakeholders with appropriate, secure, resilient, two-way interaction at the local, state, and federal (civilian and defense) level. This capability would connect and enhance but not replace mission-specific state and local emergency management, law enforcement, defense, and other systems and mechanisms, including EOCs, Special Operations Centers, Law Enforcement Intelligence Operations, Dispatch Centers, etc.

This pilot project would provide a model which could be customized by states and localities across the nation.

Background

Since the September 11 attacks more than five years ago, acquiring information on threats to infrastructures, vulnerabilities, and impacts has been a top priority and essential for determining CI/KR criticality and risk. At the national level, sector-focused Information Sharing and Analysis Centers (ISACs) were established. As understanding grew of infrastructure interdependencies and the need for identifying asset criticality and managing disasters, regional public-private partnerships emerged in some parts of the country. A major objective of these partnerships was to facilitate regional information sharing by building trust among key stakeholders and cooperatively identifying security and preparedness gaps.???

At the same time, in states and municipalities nationwide, law enforcement authorities created information and intelligence sharing and analysis mechanisms to focus on threats and crimes. Today there are more than three dozen of these information fusion centers in various stages of development and reflecting the cultural and jurisdictional interests of the areas they serve. Their goal is to develop the technologies, procedures, analytic staff and capabilities to integrate and assess relevant law enforcement and intelligence information, coordinate security measures, and facilitate two-way flow of timely, accurate, actionable information on all types of hazards. The focus, scope, functions, participation, and organizational structure of these centers are evolving as understanding of the requirements increases. A series last year of four Information Fusion Center Regional Conferences sponsored by Department of Justice with the U.S. DHS for managers of state and local Centers identified many issues that remain to be resolved. Some of the more important of these issues are:

- Expanding the focus of the Centers to cover all threats, all crimes, and all hazards;
- Inclusion of critical infrastructures and essential service providers and other key stakeholders with focus on two-way information-sharing;
- Creating and maintaining regional situational awareness pre and post incident; and
- Outreach to communities, including associations serving ethnic and special needs groups.

A priority issue is developing a *virtual capability* (i.e., procedures, technologies, organizational structure, and supporting concept-of-operations) to link information fusion centers and other collaborative mechanisms and key stakeholder organizations in a state-wide or broader regional interoperable network to accommodate diverse multi-jurisdiction needs, geographic realities and cultural and infrastructure sector interests. This virtual Regional Information Fusion Center would have two-way information sharing based on a multi-layered secure and resilient system with analysis produced by a team of core resident local and state experts and virtual analysts from different sectors and disciplines using a largely virtual database to enable integration, assessment, and secure, tailored dissemination of information provided

to key stakeholders. This analysis would be used for organizational and collective decision-making and crafting public information.

This virtual capability will interconnect state, local, private sector and other stakeholder capabilities while avoiding of duplication of effort, proliferation of analytical products, and competition for scarce analytical staff resources. It will also enable federal authorities to have a single focal point for effectively and securely providing intelligence and other sensitive information to a wide range of "customers".

Activities within Washington State that Can Be Leveraged

Washington State is well ahead of many other regions in the nation with an established information fusion center operated by the State Patrol and situated in the FBI Building in Seattle. The WAJAC is in the beginning stages of bringing in private sector analysts. At the local level, King County with surrounding counties have been developing regional preparedness plans and working with key stakeholders to address vulnerabilities and impacts associated with infrastructure interdependencies.

A public-private Partnership for Regional Infrastructure Security has been in existence since 2002. There have been four regional interdependencies exercises developed and conducted by the Partnership thus far, each focusing on a different type of threat scenario—physical and cyber attacks/disruptions, natural disasters (subduction zone earthquake) and an influenza pandemic. These exercises have resulted in recommendations for creation of a Regional Information Sharing and Analysis Center (regional ISAC) to enable key stakeholders to prepare for and manage disasters from terrorist attacks, natural disasters or other causes. In addition, Partnership members are currently testing an automated interdependency template developed for them by DHS/S&T/CIP and have created an Information Sharing Working Group to develop secure information sharing procedures for private sector organizations to exchange agreed interdependencies data collected internally with the template.

There is a community-focused alert and warning system, NWWARN, and the City of Seattle and King County are looking towards developing an information fusion capability to serve local law enforcement needs that would include critical infrastructures and essential service providers. Various proposals and some work are underway on enhancing these existing capabilities. The City of Seattle Police Department and the Pacific Northwest Laboratory have been collaborating on technology and procedural requirements for a Seattle/King County regional fusion center. ESRI is developing a virtual analysis system for use by fusion centers. There are plans to enhance WAJAC's collection, analysis, and dissemination of information and intelligence to law enforcement and non-law enforcement agencies through developing effective Regional Intelligence Groups (RIGS) and creating a Threat Early Warning Group (TEW) system.

Pilot Project Overall Goal

The goal of the proposed pilot project is to develop a statewide virtual regional cross-sector, cross-jurisdiction, secure, and resilient two-way information sharing capability that:

- Protects proprietary data;
- Utilizes existing procedures and mechanisms;
- Focuses on all threats, all crimes, and all-hazards;
- Identifies vulnerabilities, security and preparedness gaps, and assesses risk;
- Meets local law enforcement needs;
- Has a state-wide scope and reaches outside state boundaries and cross-border to address regional interdependencies;
- Supports the alert and warning function of NWWARN and incorporates member organizations as appropriate;
- Supports Emergency Operations Center Disaster Management Activities;
- Undertakes outreach and educates community groups;
- Fosters interoperability and standardization;
- Provides federal agencies through a single focal point access to state, local, and regional key stakeholders.

Tasks

The following tasks and subtasks need to be accomplished for a Regional Information Fusion Center Pilot Project. Some are already underway. Most can be addressed simultaneously *Specifics on how to accomplish these tasks and subtasks, including a schedule and milestones, will be developed by a* **Regional Information Fusion Requirements Task Force** ***comprised of representatives of organizations involved in the current information sharing and analysis activities noted in the Background Section of this paper and others as appropriate. (Duration of project activities is dependent on technical expertise/funding available.)***

Task 1: Requirements Definition ***(Six-months duration)***

1.1 Identify local, state, and federal jurisdictional issues and needs and what memorandums of understanding and other agreements are required;

1.2 Develop framework for a mechanism to integrate funding streams for Fusion Center sustainability;

1.3 Identify roles and responsibilities and develop decision-making process;

1.4 Determine membership criteria—what critical infrastructures and essential service providers to include and how to develop sector and organizational collaboration arrangements to enable collective information sharing;

1.5 Identify security and proprietary data protection and control needs and develop/leverage appropriate procedures and systems, e.g., PCII;

1.6 Develop requirements for creating (or leverage an existing) virtual information sharing system with access based on multiple levels of security that enables stakeholders to provide and receive data virtually (i.e., virtual database, analysis and dissemination);

1.7 Identify what data (information and intelligence) should be collected, which organizations will provide it and how;

1.8 Determine the security levels for data required and what security safeguards are required;

1.9 Ascertain data storage needs—what types of data can be stored, and how and where stored;

1.10 Determine information assessment needs—customer base, types of analysis required meeting customer requirements, and data and analytic resources necessary;

1.11 Determine communications and IT security requirements

1.12 Determine communications and IT resilience needs

1.13 Determine what analytic tools are needed to identify and assess regional interdependencies and disruption impacts; also for weapons of mass destruction (WMD) detection and impacts analysis, including users of these tools;

1.14 Develop requirements for a virtual analytic capability (determine qualifications of experts, security requirements, process, and procedures);

1.15 Determine Pilot Project oversight process and program management;

1.16 Identify potential sources of funding and how to acquire necessary support.

Task 2. Implementation (multi-year scope—phases and timeframe TBD)

2.1 Develop a Concept of Operations for the Regional Fusion Center that includes decision making and information sharing protocols and secure dissemination procedures;

2.2 Develop procedures for providing security clearances to Center staff and key stakeholder personnel as appropriate;

2.3 Develop training for Fusion Center personnel and analysts (working with DHS/IA);

2.4 Develop procedures and provide staff training for Community Outreach;

2.5 Develop Regional Information Fusion Center systems and tools;

2.5.1 Data collection system;

2.5.2 Data storage and virtual data system;

2.5.3 Assessment "toolset";

Task 3. Issues Investigation, Test, Evaluation and Validation (timeframe TBD)

3.1 Hold targeted workshops and exercises to further investigate and refine implementation issues and priorities;

3.2 Test and evaluate the Regional Information Fusion Center through two to three Blue Cascades regional infrastructure interdependencies exercises that have terrorism and regional disaster scenarios.

3.3 Develop and conduct additional targeted workshops and exercises to evaluate specific Regional Fusion Center capabilities.

Ms. HARMAN. Mr. Stein.

STATEMENT OF STEVEN L. STEIN, SENIOR PROGRAM MANAGER, PACIFIC NORTHWEST NATIONAL LABORATORY

Mr. STEIN. Thank you Madam Chair, Congressman Reichert, Congressman Dicks.

It is a pleasure to be here representing the Pacific Northwest international laboratory.

I actually find myself probably in the perfect chair because I'm in vital agreement with the prior two witnesses.

The beauty of the position I'm in is that I'm kind of being an observer. I'm not really government. I'm not really private sector.

My exposure to this issue has been through the regional technology abrasion initiative which is supported by the Department of Homeland Security, science and technology side.

The beauty of that program, in my opinion, is that, as you stated earlier, it starts from the ground up.

The purpose was to meet with the people who live with the problems and talk about the challenges before them, and based on their expertise and their wisdom, identify the challenges to them.

That's the position I've been in for the last four years in this region, and it has truly been an honor and a blessing, and I've learned a lot in the process.

One of the things that was keyed up in that process was that prevention and preparedness was a key element in this region.

A lot of money was being put into emergency response, but prevention was one of the pieces that wasn't as keenly reenforced.

The law enforcement in the region stepped up and said, "We need to doing something about that," and regionally they decided to go ahead and move forward with the regional community intel center.

I've had the opportunity to continue to participate in that.

One of the challenges with a regional intel fusion center or a fusion center at a state level is that partnership between law enforcement, and we've all talked about trust, but also that relationship with industry.

The partnership with industry—I really don't need to talk much about that. It's clearly beneficial. It's clearly important. The challenge though is who do you bring into the room, what's that company that you bring into the room, and then what's their obligation and liability.

What appeared to me through this process is that NWWARN actually is a phenomenal vehicle, wasn't created for this reason, but it provides, as Matt indicated, that trust in network, the vetted partnerships, the vetted participation, a secure portal, all of which allow connectivity within the infrastructure and between them and law enforcement, if this is connected to a fusion center.

The beauty is that industry doesn't have to sit inside the fusion center.

All of the things that they would through NWWARN that they can do, and that information that can be piped into the fusion center, and literally run the background—you can run information systems over the top of that, you can identify commonalities, you can identify correlation, and as you find those needles in the haystack, you can then investigate those and, as appropriate, feed back through the same channel information that's relevant to industry or that sector so that they can take the necessary action to both be prepared and prevent issues in their infrastructure, so everybody is tuned in, everybody's advised, everybody is aware, without

having to deal with the political issues, and without struggling with the timely issues.

The intelligence is great if it's timely. It doesn't do anybody any good if it's not.

This process allows that all to occur in real-time. It provides a two-way flowing of information. It doesn't create problems with security. It doesn't disappear and everybody is vetted in the system. The trust is there.

One of the other things that's really, really powerful about this, in my opinion, is that it is absolutely scale. You can do it in a small jurisdiction. You can use the same mechanisms that you would in a very large jurisdiction.

It provides the opportunity for you then to connect fusion centers to fusion centers and create a network across the country that is truly robust.

With that, I would like to thank you and would be delighted to answer any questions.

Ms. HARMAN. Thank you, Mr. Stein.

[The statement of Mr. Stein follows:]

PREPARED STATEMENT OF STEVEN L. STEIN

Mr. Chairman and members of the subcommittee, thank you for the opportunity to share some of my views on information sharing between state and local law enforcement and the private sector.

Introduction

In 2004 Pacific Northwest National Laboratory was asked by the Department of Homeland Security, Science and Technology to lead the Regional Technology Integration Initiative (RTII) for the Seattle Urban Area. In leading this effort I have had the pleasure and honor of working with hundreds of professionals in the public and private sectors who are committed to public safety and the protection of their communities. The first phase of this program was to work with the public safety sector and private sector to identify the major technology gaps that if met, would significantly improve regional preparedness for major disasters whether natural or human induced. One of the key findings of this program was that the Seattle Urban Area Emergency Management Planners should direct more resources into prevention. Regional law enforcement used this platform to pursue the development of a Regional Fusion Intelligence Center that would focus on intelligence lead, community policing. This effort is being coordinated with the state intelligence fusion center.

Regional Intelligence Fusion Center

At its origin the Regional Intelligence Fusion Center was conceived as a partnership. Regional law enforcement recognized that their focus on jurisdictional priorities and boundaries was self limiting. They also recognized that resource limitations resulted in suboptimal intelligence capability. The fundamental question then was how do you improve your operations and get the desired results without a significant and sustained increase in resources? The answer is to partner.

The vision for this partnership is that it will be a multi-jurisdictional and multi-disciplinary organization with representatives from state, local, federal and tribal partners, all working toward common objectives. At a minimum, it will include the regional intelligence groups in Pierce, Kitsap, King, and Snohomish Counties, the intelligence operation in the Seattle Police Department, and local industry. Federal law enforcement agencies and the Washington State Fusion Intelligence Center are also envisioned as partners as is the Pacific Northwest National Laboratory, Public Health, Fire, Utilities, and the private sector.

Without leadership, an articulation of the challenges that need to be overcome, and a critical mass of supporters to articulate and improve the concept, this partnership would never have moved forward. Although there are, and will continue to be numerous challenges I would like to focus my remarks on information sharing with the public/private sector.

The Northwest Warning, Alert & Response Network (NWWARN)

The benefits of information sharing between the public and private sector are well recognized. The challenge for any Regional Intelligence Fusion Center is not how to build the partnership with the private sector but rather, who should that partnership be with and what kind of information should be shared? The attributes of an ideal solution include:

- Trusted network of public/private sector representatives by infrastructure element
- Vetting of participating members so only qualifying individuals are allowed to participate
- Defined roles and responsibilities for private sector members
- Secure communication portal for information sharing

The Northwest Warning, Alert & Response Network (NWWARN) has all these attributes making it a very attractive solution to the challenge of information sharing between the public/private sector and law enforcement. The NWWARN was established as a pilot project of the Department of Homeland Security's Homeland Security Information Network—Critical Infrastructure. NWWARN, a collaborative effort between government and private sector partners within Washington State, has as its goal, to maximize real-time sharing of situational information and provide immediate distribution of intelligence to those in the field who need to act upon it. Information sharing occurs through a secure web portal and within each infrastructure element. Members are vetted by knowledgeable individuals within each infrastructure element, ensuring the formation of trusted network.

Although initially established to allow infrastructure elements to communicate with one another in an emergency, NWWARN became an effective information sharing vehicle for a range of issues. Establishing an information sharing partnership between NWWARN and the Regional Fusion Intelligence Center would not change the purpose or operation of NWWARN. Rather, it enables regional law enforcement to collect and analyze the information NWWARN members provide to each other on a daily basis. If law enforcement analysis reveals patterns or suggests heightened awareness, law enforcement can use the NWWARN network and secure portal to immediately share appropriate information with the potentially affected infrastructure elements.

Conclusion

As I mentioned at the beginning, it is a pleasure and an honor to be able to work with the law enforcement organizations in the region. The vision for a Regional Intelligence Fusion Center in the Seattle Urban Area is moving toward reality. The existence of the NWWARN offers an ideal conduit to enable information sharing between the public/private partners and regional law enforcement.

Ms. HARMAN. Mr. Stevenson.

STATEMENT OF RICHARD H. STEVENSON, PRESIDENT AND COO, CLISE PROPERTIES, INC.

Mr. STEVENSON. Thank you, Madam Chair and committee members.

Good afternoon. I'll be brief. It's Friday afternoon.

My name is Richard Stevenson. I'm president and chief operating officer of Clise Properties, Inc., a 120-year old commercial real estate company with approximately 3 million square feet of commercial space, mostly located in the downtown core of Seattle.

I'm also a past chair of BOMA, building owners and managers association of Seattle and King County, current board member of the downtown Seattle association, board member of the housing resources group and also the downtown emergency services center.

I've managed commercial property and commercial real estate companies in the Seattle area for approximately 27 years.

Generally speaking, during that time I believe that those of us in the industry have formed a very strong relationship with local law enforcement and specifically with that of the Seattle police department.

My first real professional interaction with SPD was in or around 1991 when businesses located on 1st Avenue near the Pike Place

Market formed a business improvement area for the purposes of managing street issues: Cleaning, pan handling, et cetera.

The then west precinct commander, Captain Clark Kimerer, agreed to a formal interaction between our security patrols and the west precinct for the purposes of communicating issues common to the business improvement area's goals and that of Seattle's downtown west precinct.

This, at the time, was very bold and innovative thinking.

Since that time we've had a close working relationship with the police department as it relates to emergency response, sharing of information, and oftentimes on a street level having individual officers have access to the buildings for purposes of surveillance, occasional access to restrooms for bicycle police, and other operational issues.

I'm here today in front of you because it's my feeling that with regard to homeland security, we would prefer to see their efforts and resources used to bolster local law enforcement on our behalf as opposed to standing alone in potentially duplicate service.

We would hope that in local law enforcement and homeland security there would be a type of communication between entities needed to provide us with intelligence, financial resources, manpower, and technology to provide safety for our downtown commercial office buildings and the vitally of the urban core as a whole.

What I mean by this is that I believe the local law enforcement, including our relationships with ATF, FBI, and others, have provided us a strong and reliable core, and then I think their efforts should be furthered buttressed by a federal homeland security funding for vital infrastructure improvements that are mutually agreed upon by the various parties.

It would seem to be a mistake for Homeland Security or any other governmental agency to go it alone in Seattle when it could act as a valuable supporting team member for an existing and functional local private relationship.

The excellent relationship between the downtown business community and the Seattle police department has been the result of years of collaboration on the real world challenges.

We worked together for many years at ground level. Our relationships have been tested and retested over time.

The key to our success has been a thorough understanding of our respective roles and responsibilities.

The private sector does not want to take on the role of law enforcement. We want to be informed, consulted, and provided timely warnings. In return we will lend our support and assistance to law enforcement as they perform their duties.

We have valuable information and insights into the strengths and vulnerabilities of the buildings we own and manage, and are at the table when public safety and homeland security priorities are debated by our elected officials.

I have every confidence that Chief Kerlikowske and Deputy Chief Kimerer will give me the information we need if threats are identified, and I believe that they are confident that Clise Properties and our colleagues in the downtown business community will do everything that is in their power to assist the police department.

This has been a model relationship, and it is only possible at the local level because of our frequent and ongoing interaction in the course of our daily business.

Thank you.

Ms. HARMAN. Thank you very much.

[The statement of Mr. Stevenson follows:]

PREPARED STATEMENT OF RICHARD STEVENSON

Good afternoon. My name is Richard Stevenson. I am president and chief operating officer of Clise Properties, Inc., a 120 year old commercial real estate company, with approximately 3 million square feet of commercial space, mostly located in the downtown core in Seattle.

I am also a past chair of the Building Owners and Managers Association of Seattle and King County and a current Board member of the Downtown Seattle Association, Housing Resources Group, and the Downtown Emergency Services Center.

I have managed commercial property and commercial real estate companies in the Seattle area for approximately 27 years. Generally speaking, during that time, I believe that those of us in the industry have formed a very strong relationship with local law enforcement and specifically with those of the Seattle Police Department.

My first real professional interaction with SPD was in or around 1991 when businesses located on First Avenue, near Pike Place Market, formed a Business Improvement Area for the purposes of managing street issues, including cleaning, panhandling. The then West Precinct Commander, Capt. Clark Kimerer, agreed to a formal interaction between rented security patrols and the West Precinct for the purposes of communicating issues common to the business improvement area's goals and that of the Seattle's downtown West Precinct. This, at the time, was very bold and innovative thinking. Since that time, we have had a close working relationship with the Police Department as it relates to emergency response, sharing of information, and often times on a street level, having individual officers having access to buildings for the purposes of surveillance, occasionally access to restrooms to bicycle police, and other operational issues.

I am here today in front of you because it is my feeling that with regard to Homeland Security, we would prefer to see their efforts and resources used to bolster local law enforcement on our behalf as opposed to stand alone and potentially duplicate services. We would hope that between local law enforcement and Homeland Security there would be the type of communication between entities needed to provide us with intelligence, financial resources, manpower, and technology to provide safety for our downtown commercial office buildings and the vitality of the urban core as a whole.

What I mean by this is that I believe local law enforcement including their relationships with ATF, FBI and others have provided us a strong and reliable core and I think their efforts should be further buttressed by a federal homeland security funding for vital infrastructure improvements that are mutually agreed upon by the various parties. It would seem to me a mistake for Homeland Security, or any other governmental agency to go it alone in Seattle when it could act as valuable support and a team member for an existing and functional local public private relationship.

The excellent relationship between the downtown business community and the Seattle Police Department has been the result of years of collaboration on real world challenges. We worked together for many years at ground level, and our relationships have been tested and retested over time. The key to our success has been a thorough understanding of our respective roles and responsibilities. The private sector does not want to take on the role of law enforcement. We want to be informed, consulted and provided timely warnings. In return, we lend our support and assistance to law enforcement as they perform their duties. We have valuable information and insights into the strengths and vulnerabilities of the buildings we own and manage, and are at the table when public safety and homeland security priorities are debated by our elected officials. I have every confidence that Chief Kerlikowske and Deputy Chief Kimerer will give me the information we need if threats are identified, and I believe they are confident that Clise Properties and our colleagues in the downtown business community will do everything within their power to cooperate and assist the police department This has been a model relationship, and is only possible at the local level because of our frequent and ongoing interaction in the course of our daily business.

Ms. HARMAN. The last two of you finished in less than two minutes. I commend you. You get the gold star.

As I mentioned, your testimony will be inserted in the record in full, and each of us will now ask you five minutes worth of questions.

I'll recognize myself first.

Mr. Hovel, you mentioned the Fort Dix issue when, I think, it was six would-be terrorists were apprehended recently in New Jersey and charged with plans for a major attack on Fort Dix.

As I recall, the first notice to law enforcement came from a—I think it was a video store fellow who—or a camera store fellow who was asked to do something with a video that these fellows had prepared, and that video obviously contained material that was very alarming.

This obviously illustrates a point you've all made, which is that the private sector has a lot to contribute here, not just to keeping its own facilities safe if it gets the right information but keeping the rest of us safe.

Had that plot not been foiled, obviously there possibly could have been a major attack on a U.S. military base.

I just observe that.

If you have anything to say about that, please do, but I really want to ask a different question.

Mr. Morrison, your testimony was extremely depressing.

I have said for years that the dirtiest four-letter word in government is spelled T-U-R-F, turf, and I think that for some reason, maybe it's the water we drink, people instinctively protect power and draw perimeters around themselves—it sounds like instinctive animal behavior—and block out others.

What are the best ways to overcome turf instincts?

Do we have to legislate and force people to be different? Is there some management technique? Do we need different people?

What is it going to take to overcome turf?

Mr. MORRISON. Madam Chair, that's a pretty tough question.

I think that certainly if—in the local and regional sense it's quite possible to do.

In terms of the dysfunctionality of DHS, I don't know.

I mean, I just—anyway, it's amazing to me.

In our pandemic, we're trying to do a comprehensive regional pandemic plan and HHS has theirs and DHS has theirs, and there's—I mean, it's amazing.

Ms. HARMAN. Is it easier at a local and regional level because people know each other, live closer to each other.

Mr. MORRISON. Definitely.

Ms. HARMAN. There's common geography? What are the clues.

I'm sure there are some people here, of course nobody in this room, who are pretty protective of their own power structure and block out others, right?

Mr. MORRISON. Right.

Ms. HARMAN. No one in this room, certainly not my colleagues.

It escapes me. I am very frustrated.

I have been personally involved in the legislation to create the Department of Homeland Security, which I agree has enormous organizational issues, and to reform our intelligence community, which is still a work in progress, and the instinct is to build bureaucracies and enact procedures that aren't—that keep data in

one place and systems that are duplicative and all the things you've all been testifying to and our first panel has too, but I think we need a better approach.

Legislation by itself doesn't work. Good people try very hard, and that doesn't work. The problems are identified over and over, and that doesn't work.

Does anyone else have some ideas?

Mr. Stein?

Mr. STEIN. I don't want to get myself in trouble.

It's leadership.

I mean, there's lots of things obviously, but my observation in this community is the reason it works is because of the leadership.

The people that were here before at the earlier panel, those gentlemen tell the people that they're working with what their objectives are, what their goals are, and they walk their talk.

They re-enforce those behaviors with their peers and with their subordinates.

That leadership translates down.

Now, at the lower levels, it's far from perfect, but the message is loud and clear, and as a result you get a lot more cooperation and collaboration, and I am in that kind of unique position of not being in any of the camps, so I kind of see it in a different way.

This is where I'll get myself in trouble. In DHS, the question I would ask is: Do you have the right leadership in the context of people who see that bigger issue, that bigger objective, and are really willing to walk the talk to achieve those goals?

I can't answer it, but the observations are what you can make.

Ms. HARMAN. My time has just expired.

Does anyone else have a comment?

Okay. Well, I would just agree with you that any of these laws and any of these departments, whatever their legal basis is, are in my view about 50 percent structure and 50 percent leadership, and I do think leadership is critical.

It was an ancient Chinese philosopher, Lao Tzu, who said the more power you give away, the more power you have, and it seems to me certainly the people in Washington have never heard of Lao Tzu.

Let me now yield to five minutes for questions to the ranking member, Sheriff Reichert.

Mr. REICHERT. Thank you, Madam Chair.

Well, turf wars—I've started in the sheriff's office in 1972, and there have been turf battles since 1972 and still today.

It's the human nature, I guess, that we live with, but it does take leadership.

We had a team of leaders sitting before of us earlier and we have a team of leaders sitting before us right now, so we know in this community we have the makings of great programs, of great systems because we have people here who are interested and who are willing to work together.

So my first question goes to Mr. Hovel and Mr. Stevenson.

Your two companies, is it unique to your companies, the connection and the involvement and the interaction that you have with your local police departments and this interconnection with not just addressing local crime but the whole concept of homeland security

or are you reaching out too to other companies and building that platform to make it even stronger?

Mr. HOVEL. Mr. Congressman, we have done all of those things and in the process of reaching out to many other companies.

Obviously not all of them have the luxury of being able to participate at the level and in the manner that we are, but that being said, because we have that capability, we are not going to let the opportunity pass either, but there are many ways, as I mentioned one of in my prepared remarks, concerning the virtual network, that will go a long way to allowing those who really have an interest in participating but otherwise don't have the means or the logistics to do so to become an integral partner in this entire effort.

Mr. STEVENSON. You know, it was mentioned earlier—in fact, Chief Kerlikowske mentioned that one of the outcomes was the police association, and I think that that is a perfect example of one of the things we've been able to do locally is have business leaders, downtown Seattle association, other groups, get together, work for the police foundation, raise money.

We saw a real need.

I mean, bicycle policemen in Seattle didn't have BlackBerrys, and so they would stop somebody on the street and couldn't really figure out what to do with them, other than call a squad car and I guess run them downtown, and we got together the money, we got the BlackBerrys.

We had this very close working relationship because it's very mutually beneficial to us and it's the right thing to do, and I think we do it because we're stakeholders and we've got skin in the game, and I think they do it because they're great people and it's their job and their career and they're excellent at it, and it seems to me that the previous question that Chairwoman Harmon had was "Why doesn't it work," and I would suggest that maybe not everybody has enough skin in the game.

Mr. REICHERT. Well, I would think too that not only do you attract other businesses but you are also, in assisting the police department, the sheriff's office, and other police departments, that you have the ability then to reach out to the various diverse communities that exist around your businesses and the employees that you have within the businesses and get them involved, and it really goes back to, and the chief well knows this concept, of community policing.

It really has had to step up to the next level to have an impact on, again, that overarching concept of homeland security.

Are either of you—I should have ask the chief this. I'm sure he is. Is anyone in this panel aware of the Muslim public affairs council?

So we're involved in that effort in bringing that community together and reaching out and further educating our community? Good, good. I am glad to hear that. I wasn't quite sure.

To get back to Matt, it's good to see you. You too, Steve.

On the issue of the HSIN critical infrastructure, you testified it's closed down, and by who?

Mr. MORRISON. By the department.

They transformed it to—

Mr. REICHERT. By Homeland Security.

Mr. MORRISON. HSIN CS, which is critical sectors, which is a stove-piped, one direction only communications system, and it doesn't work for what we have in mind.

Mr. REICHERT. I have no further questions.

I yield.

Ms. HARMAN. Thank you.

Mr. Dicks is now recognized for five minutes.

Mr. DICKS. Let's stay on that subject again.

Now, P–N–W–E–R, PNWER, is your big organization, multistate, and you're the leader of that operation, right?

Mr. MORRISON. I'm just the executive director. The governors—

Mr. DICKS. Who created NWWARN?

Mr. MORRISON. That was a joint effort between the Seattle FBI, PNWER, and our stakeholder group.

Mr. DICKS. So it's separate from your organization—

Mr. MORRISON. DHS, FBI, and we petitioned to DHS at the time to be a—

Mr. DICKS. And at first they brought you into the fold, right.

Mr. MORRISON. That's right. This was 2000—

Mr. DICKS. And this was based on the Dallas, TX emergency response network, ERN, which was largely a law enforcement focused model out of the Dallas FBI.

Mr. MORRISON. Right.

Mr. DICKS. And it was after much delay, isn't that correct, that DHS agreed to let you be part of the new model, which became known as HSIN critical infrastructure or HISN CI.

Did this letter that went out to the 2,000 people that were involved in this operation, did you know they were going to go out or did they just all of a sudden everybody gets this letter saying this is being disbanded?

Mr. MORRISON. That's right.

Mr. DICKS. Is that how it worked.

Mr. MORRISON. That's how it worked.

Mr. DICKS. Why did they do it?

Mr. MORRISON. I have no idea.

Mr. DICKS. Have you talked to any of them.

Mr. MORRISON. Yeah, I mean, we have.

It was a turf battle going on between FBI and DHS, even though they're both DHS, but it—

Mr. DICKS. You know what I would have done? I would have called my congressman or your senator or somebody and asked for some help.

Could you do that? Have you asked anybody to help you?

Mr. MORRISON. Oh, yeah.

I mean, we have, but maybe not as effectively as we could have.

Mr. DICKS. I think these—like your Blue Cascade things, I think those—I think we should be holding you up as the model for what a regional entity ought to be doing.

I mean, cyber systems, earthquake preparedness, pandemics, these are the kinds of things we need to be doing, a possible attack on BPA assets—those are the four, aren't they?

Mr. MORRISON. Yes.

Mr. DICKS. I mean, I would think that the federal government would think this is what a regional group should be doing.

I am really taken aback by this, that this—when did this happen?

When did these 2,000 letters go out?

Mr. MCKAY. It was March 21.

Mr. DICKS. I am certainly, as a member of this committee, I'm going to bring up the DHS people and get an explanation for this, and any information you can give me about the whole thing, I would appreciate it because I don't think this is right, and I certainly want to find out why they did this.

I think—I think you're right, the sector idea, the chemical industry, all of these various industry groups, and they're supposed to come up with industry recommendations. That's been going very tediously as well, by the way. That hasn't been an example of moving out and getting something done, is it?

I mean, have you—

Mr. MORRISON. The secretary announced this week that the sector specific plans are now released, six months late, but they are out this week.

Mr. DICKS. Has anybody had a chance to look at them? Are they any good.

Mr. MORRISON. Well—

Mr. DICKS. See I like—sector specific, I like the idea of a regional approach because that way you know—you've got all the various institutions in that region that are effected, and I would love to have some of the information on your Blue Cascade, these four exercises that you did, because I think those are where you really learn where the vulnerabilities are and what the problems are, and if you could get that to us, I would definitely—I'm sure our committee would like to have that to take a look at.

Mr. MORRISON. We would love to testify in Washington about them, but I think for me it was with General Lowenberg one time who said, "DOD told me all the vulnerabilities in Washington state. DHS told—you know, in five days, but something is in the top five was on neither list, and I wouldn't know about it if I wasn't at the blue Cascades exercise."

Mr. DICKS. Yeah. One of the things that he found out about the cyber security issue, right, wasn't that it.

Mr. MORRISON. I'm not going to say anything—

Mr. DICKS. That was the one, I believe.

You know, when they first came out, when Homeland Security first came out with their critical infrastructure in the state of Washington, do you know what two businesses were not on the list? Boeing and Microsoft.

I mean, can you imagine having a list—I took one look at this list, and I just said, "I mean, this cannot be true," and it was true.

I don't know. They had a number of recreational places and things like that, but they didn't have Boeing and Microsoft on the list of critical infrastructure in the state of Washington, and we got that straightened out, and—I just—we've got to do better, and I appreciate all your testimony today and the work that you're all doing, and we'll—all of us here on a bipartisan basis, we all work together. This is about finding some answers.

We're going to help you try to find some answers on these issues.

Thank you.

Ms. HARMAN. Thank you, Mr. Dicks.

I want to thank the witnesses for your valuable testimony.

The lively discussion obviously keys off of what you had to tell us. Some of it was very depressing. Some of it is inspiring us to action.

You have in these two members people who want to fix these problems and are obviously very proud of their home state, as they should be.

I would just mention to Mr. Dicks, and I think he knows this, that a lot of the information about critical infrastructure is classified, and there's a place where I actually think it ought to be classified.

We don't need to be telling the bad guys what our major vulnerabilities are, but we surely do need to get proper lists that reflect the activities of states.

There was a very foolish list for a long time that had golf courses—not that golf courses aren't important, but I don't think even golfers would claim—well, my husband would claim that they're critical infrastructure, but seriously, I think those lists do need to be kept classified, but I think your point is very well taken that we have to integrate the list.

We can't have more stove-pipes—again, that seems to be our tendency to have all these separated reports.

If I were Michael Chertoff, I would perhaps be inspired, after hearing this information, to try to infuse his department with more coordination and more of a shared mission than it has.

Mr. DICKS. Madam Chairman, they're not helping us very much.

Ms. HARMAN. And something that we have just decided to do is sit down privately with him and go over our top ten list—some of those top ten have just come out of this hearing—of things that we think he needs to work on, and rather than making it confrontational, we'll just have it be a conversation, and maybe that is a key to getting some of this fixed.

Surely he doesn't bring all of this turf consciousness to his job. It's in the woodwork and it was in the woodwork of the 22 different agencies we thought—we in Congress decided we could put into one organization on a quick basis, so that is a problem.

Mr. Reichert has asked me to thank the mayor of the City of Bellevue.

I think I recognized him at the beginning of the hearing, but I would like to thank him again for making this facility available, and just say to all of you that you are a model, and Mr. Dicks is right that we need to bottle you in some fashion and make sure that the good work you've done here is encouraged and nurtured and spread around the country.

It does occur to me that places that are well organized, like Washington state and the Los Angeles county area, have a lot to teach the rest of the country.

We're not exactly the same as other parts of the country, but in terms of coordination in difficult circumstances, we are a very good model, and best practices matter.

We're spending a lot of money on this. I'm sure we could spend more, but we need to spend it wiser than we do.

Let me just finally say that something else that was not mentioned today that is critically important to fix is interoperable communications, and I worry a lot that should we have another major terrorist incident, and I believe we could have one at any time, we might have the same meltdown that we had in New York and Washington again in some community or some set of communities around the country, so there's a lot of work to do.

All three of us care a lot about this, and I would like to ask both members if they have any concluding remarks, starting with Mr. Reichert.

Mr. REICHERT. Thank you, Madam Chair.

I just want to end on a real positive note in honor of our dear friend Norm.

We have talked a lot about turf wars. Norm recognized those. He and I talked a lot about those as well as most of you in this room had the opportunity to work with Norm, but he had two favorite things that he would always share with people, and maybe some of you in this room even heard him say these words to you.

One was if he would come to you and ask you how you were doing, and you said, "You know, I'm doing okay, Norm," he would say, "You know what, we need to move ahead today with a smile on our face and an optimistic spirit," so we can do that when it comes to these problems.

The second thing, Norm would come to me and now and then we would visit and talk, and I remember one day a really challenging issue in the sheriff's office, and I told him I had this challenge ahead of me, and he said, "You know, Dave, there's no such thing as a challenge, only opportunities," so today we have opportunities, and we've got a great team.

We really have some great opportunities to do some great things and be true leaders here in our region, so I thank all of you for all the hard work that you do to keep our community safe.

I thank the chairwoman for holding this hearing in our district, and I again thank Norm for all of his hard work on behalf of our country and our community.

Thank you.

Ms. HARMAN. Norm.

Mr. DICKS. Thank you Jane for coming up and being here today with us, and Congressman Reichert and I have been working on this.

Last Congress, the Congressman was chairman, and I told him that he got to be chairman in his first term and it only took me 16 to become chairman, so—

Ms. HARMAN. Some people are slower than others.

Mr. DICKS. It took me a long time, but we're there, but again I want to thank all of you and especially General Lowenberg who has been right there at the start of this whole thing, and we want to try to help you find some solutions to these opportunities, as Congressman Reichert said, and I would just say also that Norm Maleng was a friend of mine as well, and we were in law school about the same time, and he also worked for Senator Magnuson.

That may not be well remembered, but he was on the staff of the Senate commerce committee.

The senator picked probably one of the outstanding students each year—actually it was the faculty that picked—to send back for this one-year opportunity to work on the Commerce committee, and Norm Maleng was one of those that was selected, and we all admired his career and as the prosecuting attorney in King County for so many years, and so many important things that he accomplished, and we're going to miss him, so thank you.

Ms. HARMAN. Thank you, and finally let me thank the bipartisan staff of the Homeland Security Committee.

This hearing is adjourned.

[Whereupon, at 2:58 p.m., the subcommittee was adjourned.]