

Critical Infrastructure Partnership Advisory
Council (CIPAC)

The 2010 CIPAC Plenary

October 13, 2010
The Hyatt Regency Bethesda
7400 Wisconsin Ave
Bethesda, Maryland

Meeting Transcript

RENEE MURPHY: Good morning, if you would please take your seats we will begin the 2010 CIPAC Plenary. CIPAC has been exempted from Federal Advisory Committee Act reporting requirements. In light of this exemption and as a matter of policy, the Department of Homeland Security operates the CIPAC in a manner consistent with the spirit and principal of transparency. This plenary meeting is open to the public, but it is only one way of implementing transparency. The other is the publication of notices and information on CIPAC meetings on the Department of Homeland Security's web site. As today's meeting is open to the public, members should exercise care when discussing potentially sensitive information.

I will now conduct the sector roll call. If you will please indicate if you are present:

RENEE: Banking and Finance, GCC, SCC.

MARLENE ROBERTS: GCC present.

RENEE: Chemical, GCC, SCC.

AMY GRAYDON: GCC present.

BILL ALLMOND: SCC present.

RENEE: Commercial Facilities, GCC, SCC.

DAVE CRAFTON: GCC present.

JOE DONOVAN: SCC present.

RENEE: Communications, GCC, SCC.

MIKE ECHOLS: GCC present.

ROBERT MAYER: SCC present.

RENEE: Critical Manufacturing, GCC, SCC.

KATHLEEN NUCCETELLI: GCC present.

KATIE MCCALL: SCC present.

RENEE: Dams, GCC, SCC.

KRISTEN BAUMGARTNER: GCC present.

HAL DALSON: SCC present.

RENEE: Levees, SCC.

SUSAN GILSON: SCC present.

RENEE: Defense Industrial Base, GCC, SCC.

MIKE MCDANIELS: GCC present.

BILL ENNIS: SCC present.

RENEE: Emergency Services, GCC, SCC.

KORY WHALEN: GCC present.

SHAWN KELLEY: SCC present.

RENEE: Energy, GCC.

KENNETH FRIEDMAN: Energy GCC present.

RENEE: Electric, SCC.

MARK WEATHERFORD: Present.

RENEE: Oil and Natural Gas, SCC.

JAY MONTGOMERY: Present.

RENEE: Food and Agriculture, GCC, SCC.

LEEANNE JACKSON: GCC present.

RANDY GORDON: SCC present.

RENEE: Government Facilities, GCC.

MARGARET WRIGHT: GCC present.

RENEE: Information Technology, GCC, SCC.

THAD ODDERSTOL: GCC present.

GUY COPELAND: SCC present.

RENEE: Healthcare and Public Health, GCC, SCC.

STEVE CURREN: GCC present.

ERIN MULLEN: SCC present.

RENEE: National Monuments and Icons, GCC.

CHARLES FRANKLIN: GCC present.

RENEE: Nuclear, GCC, SCC.

MARK BROOKS: GCC present.

VIJAY NILEKANI: SCC present.

RENEE: Postal and Shipping, GCC.

BOB DVONCH: GCC present.

RENEE: Transportation, GCC.

DOMINIQUE GILBERT: GCC present.

RENEE: Maritime, GCC, SCC.

ELEANOR THOMPSON: Maritime GCC present.

SUSAN MONTEVERDE: Maritime SCC present.

RENEE: Aviation, SCC.

CHRIS BIDWELL: Aviation SCC present.

RENEE: Highway Motor Carrier, SCC.

BOYD STEPHENSON: Highway Motor Carrier SCC present.

RENEE: Mass Transit, SCC.

RENEE: Rail, GCC, SCC.

GIL KOVAR: GCC present.

TOM FARMER: SCC present.

RENEE: Pipelines, SCC.

RAY REESE: SCC present.

RENEE: Water, GCC, SCC.

CYNTHIA DOUGHERTY: GCC present.

DON BROUSSARD: SCC present.

RENEE: This now concludes the sector role call. I now turn the floor to our Assistant Sectary, Mr. Todd Keil.

TODD KEIL: Thanks Renee and thank you everybody for showing up this morning. Appreciate you all taking the time. I know everybody's time and resources are valuable.

It is an honor and a privilege for me to be here with you this morning. Since I was appointed Assistant Secretary for Infrastructure Protection at the end of last year, I have come to appreciate the great importance of the public-private partnerships and of the CIPAC in particular. It is through this vital, unprecedented partnership that some of the most important work in securing our nation's critical infrastructure is carried out.

In the past years, the CIPAC plenary was a meeting that was focused almost entirely on annual activity updates. This year's plenary however will be more interactive and will feature panel discussions about crosscutting topics that are of great importance to all of us. Moreover, today's plenary session provides us with the opportunity to reflect upon the progress we have made in critical infrastructure security since the formation of this group and discuss a vision for

what more we can accomplish together. It is through our cooperative work that we are able to best understand what needs to be done to secure the nation's critical infrastructure and how to best do it.

I would like to take a moment to, even though Renee just did the role call, I would like to take a moment to recognize the people in attendance today who commit so much time and effort to protecting the homeland. If you are a member of one of the following councils, please stand and remain standing so that you can be recognized:

- Please stand if you are a member of a Sector or Government Coordinating Council.
- Members of the Cross Sector Coordinating Council.
- State, Local, Tribal, Territorial Government Coordinating Council.
- The Federal Senior Leadership Council.
- And the Regional Consortium Coordinating Council.

As you look around the room, each of you are examples of citizens who voluntarily work together to keep this country safe and I thank you for all that you do. And I appreciate, as I am sure everybody in this room appreciates the work that you do on behalf of our country. Thank you.

I think today is another example of our partnership leaning forward. As I mentioned, rather than just reporting out our activities and partnerships, today's meeting will consist of two interactive roundtable discussions that focus on the future of critical infrastructure security. The theme of the first roundtable is interdependencies and regionalization and the theme of the second roundtable will be information sharing and cyber security.

Each roundtable discussion will include remarks from panelists who represent a diversity of roles, responsibilities, and viewpoints. These important discussions will help us better understand the needs and ideas of both the public and private sector. I believe they will challenge us to do more.

Before we get there, however, we are waiting for the Deputy Secretary to arrive so that she can open the CIPAC and, Brian, do we have any idea? Probably I think it is best to rather than introduce the Deputy Secretary without her being here, I know she is in route and should be only a few minutes away, why don't we just sit back and relax for a couple minutes. So we will just wait a few minutes for the Deputy Secretary and then I will introduce her so she can give her opening remarks.

TODD KEIL: In the interests of camaraderie and in addition to the roll call, even though the roll call was by Sector Coordinating Council, Government Coordinating Council or other bodies, maybe it would be helpful for everybody if we went around the room and you introduced yourselves personally. So if you want to start at go to the right side and my right side and roll around, introduce yourselves.

CHUCK FRANKLIN: Chuck Franklin, I'm with the Department Of The Interior, representing the SSA, Sector Specific Agency for National Monuments and Icons.

MARGARET WRIGHT: Margaret Wright from Federal Protective Service, representing the Government Facilities Sector, SSA.

SEAN KELLEY: Shawn Kelley from the International Association of Fire Chiefs, representing the Emergency Services Sector.

KORY WHALEN: Kory Whalen, Department Of Homeland Security, Office of Infrastructure Protection, Emergency Services Sector.

BILL ENNIS: Bill Ennis, Defense Industrial Base, Sector Coordinating Council, Executive Secretariat representing Barry Bates.

MIKE MCDANIEL: Mike McDaniel, Deputy Assistant Secretary Of Defense for Strategy, Force Planning and Mission Assurance, representing the Defense Industrial Base, GCC.

SUSAN GILSON: Susan Gilson, the National Association of Flood and Storm Water Management Agencies, representing the Levees Subsector.

HAL DALSON: Hal Dalson, Chairman of the Dams Sector.

KRISTEN BAUMGARTNER: Kristen Baumgartner, Department Of Homeland Security, Office of Infrastructure Protection, representing the Dams Sector.

KATIE MCCALL: Katie McCall, U.S. Steel Corporation, and I'm representing the Critical Manufacturing Sector.

KATHLEEN NUCCETELLI: Kathleen Nuccetelli, Department Of Homeland Security, Office of Infrastructure Protection, representing the Critical Manufacturing Sector.

ROBERT MAYER: Robert Mayer, U.S. Telecom Association, representing the Communications Sector.

MIKE ECHOLS: Mike Echols, Branch Chief, Government Industry Planning and Management, National Communications Systems, Department Of Homeland Security.

JOE DONOVAN: Joe Donovan, Co-Chair, Commercial Facilities Sector and also BOMA's National Preparedness Chair.

DAVE CRAFTON: Dave Crafton, Department Of Homeland Security, Infrastructure Protection, Chief of the Commercial Facilities Sector.

BILL ALLMOND: Bill Allmond with the Society of Chemical Manufacturers and Affiliates, representing the Chemical Sector Coordinating Council.

AMY GRAYDON: Amy Graydon, Department Of Homeland Security, Infrastructure Protection with the Chemical Government Coordinating Council.

JANE CARLIN: Hi, I'm Jane Carlin from Morgan Stanley. And I'm the Chairwoman of the Financial Services Sector Coordinating Council.

MARLENE ROBERTS: Marlene Roberts, FDIC, representing the Financial and Banking Information Infrastructure Committee.

DON ROBINSON: Don Robinson, Department Of Homeland Security, Infrastructure Protection, Southeast Regional Director.

MATT MORRISON: Matt Morrison, Pacific Northwest Economic Region, representing the Regional Consortium Coordinating Council.

JEFFREY DELL: Jeffrey Dell, Bank of America, representing Northern California Regional Intelligence Center.

CHERRIE BLACK: Cherrie Black, New Jersey Office of Homeland Security and Preparedness and I'm representing the State, Local, Tribal, Territorial Government Coordinating Council.

KEN WATSON: Ken Watson, Cisco, and I'm representing the PCIS.

BILL FLYNN: Good morning, Bill Flynn, Deputy Assistant Secretary for Infrastructure Protection, DHS.

WILL PELGRIN: Good morning, you didn't see me sneak in, did you? Will Pelgrin, Chair of the National Council Of ISAC's. Thank you.

CLYDE MILLER: I'm Clyde Miller. I'm the Chair of the PCIS, the Cross Sector Coordinating Council and Vice Chair of the Chemical Sector Coordinating Council.

TODD Keil: Todd Keil, Assistant Secretary for Infrastructure Protection.

ULIE SEAL: Ulie Seal, I'm the Fire Chief from the City Of Bloomington. I'm Chair of the State, Local, Tribal, and Territorial Government Coordinating Council.

TOM MORAN: Tom Moran with the All Hazards Consortium, representing the Regional Consortium Coordinating Council.

JAY MONTGOMERY: Jay Montgomery, I'm the Chair of the Oil and Natural Gas Sector Coordinating Council.

KEN FRIEDMAN: Ken Friedman, U.S. Department of Energy, Office of Electricity Delivery and Energy Reliability, representing the Energy GCC.

LEEANNE JACKSON: LeeAnne Jackson, Food and Drug Administration, Co-Chair of the Government Coordinating Council for the Food And Agriculture Sector.

RANDY GORDON: Randy Gordon, National Grain And Feed Association, Co-Chair of the Food and Agriculture SCC.

STEVE CURREN: Good morning, Steve Curren with the Department of Health and Human Services, representing the GCC for the Healthcare and Public Health Sector.

AL COOK: Al Cook. I'm employed by the Regional Medical Center in Orangeburg, South Carolina. I represent the Association of Healthcare Resource and Materials Managers and I'm a Tri-Chair for the Sector Coordinating Council, Healthcare and Public Health.

THAD ODDERSTOL: Thad Odderstol, Department of Homeland Security, National Cyber Security Division, IT Government Coordinating Council.

GUY COPELAND: Hi, Guy Copeland with CSC, a past Chair of the IT Sector Coordinating Council and current Co-Chair of the Cross Sector Cyber Security Working Group. Standing in temporarily for Cheri McGuire, the IT SCC Chair who is also en route and should be arriving here momentarily. Thank you.

CRAIG CONKLIN: Good morning, Craig Conklin, Office of Infrastructure Protection, Department of Homeland Security, representing the Nuclear GCC.

VIJAY NILEKANI: Vijay Nilekani, Nuclear Energy Institute, representing the Nuclear Sector Coordinating Council.

BOB DVONCH: Bob Dvonch, the Transportation Security Administration. I'm the Director of the Postal and Shipping Sector.

DOMINIQUE GILBERT: Dominique Gilbert, Transportation Security Administration, representing the Transportation Systems Sector.

ELEANOR THOMPSON: Eleanor Thompson, U.S. Coast Guard, representing Maritime and Co-SSA within the Maritime Sector GCC.

SUSAN MONTEVERDE: Susan Monteverde. I'm with the American Association of Port Authorities, I represent the Maritime SCC, which is part of the Transportation Sector.

CHRIS BIDWELL: Good morning, Chris Bidwell. I'm with the Airports Council International North America and I'm Chair of the Aviation Sector Coordinating Council.

GIL KOVAR: Good morning, Gil Kovar, Transportation Security Administration, General Manager, Freight Rail.

RAY REESE: Good morning, I'm Ray Reese. I'm the Vice Chair of the Oil and Natural Gas Council. However for today, sitting in as representative of the Pipelines SCC under Transportation.

CYNTHIA DOUGHERTY: Cynthia Dougherty, Environmental Protection Agency, representing the GCC for Water.

DON BROUSSARD: Good morning, I'm Don Broussard. I'm the Water Operations Manager of Lafayette Utility System in Lafayette, Louisiana and I'm the Chair of the Water Sector.

TODD KEIL: Great, thank you, everybody. I am just happy we didn't have to start introducing all the people in the back of the room.

It is my distinct privilege to introduce the Deputy Secretary of the Department Of Homeland Security, Jane Holl Lute, who is going to deliver some opening remarks for us. The Deputy Secretary has served two Presidents on the National Security Council staff at the White House and has more than 30 years of military and senior executive experience in preventing and resolving international crises.

Deputy Secretary Lute has also served as Assistant Secretary General of the United Nations, where she was responsible for U.N. support to peacekeeping operations. In this capacity, the Deputy Secretary managed operational support for the second largest deployed military presence in the world. We are honored to have the Deputy Secretary with us here today to open the CIPAC plenary council.

Madam Deputy Secretary, thank you.

JANE HOLL LUTE: Thanks very much. And just for the record, it is actually three Presidents. I mention that a), because it's true and b), because it never ceases to impress on me the privilege that I have had in public service. It is, I think, an underappreciated aspect of the work that we do that we have the privilege of serving the American public. And especially since the end of the Cold War, it has been an extraordinarily dynamic environment for public policy in the United States and around the world. So thank you very much, everyone, for joining us here today.

This is an important group. It's an important representation of the partnership that the Department of Homeland Security has with the private sector in so many aspects of its work. I thought what I would touch on this morning might be familiar material to some of you. It's where the Department has been, where we are, and where we'd like to go. Within, in the context of that, I'd like to talk about the importance of partnerships, particularly in the sectors represented around this table and in this room in Critical Infrastructure.

Let me say my bottom line up front. No single agency, no federal agency, no State and local agency, I think no company or corporation can do all that needs doing when it comes to the security of the American homeland. We believe fundamentally that it takes all of us. It takes an enterprise. It takes partnerships to make this successful and when we talk about Homeland Security, what we're really talking about is how we can help make and create a safe, secure, resilient place where the American way of life can thrive. When we talk about Homeland Security that is what we are talking about, a safe, secure, resilient place where the American way of life can thrive. And over the past 20 months, we have been examining every aspect of Homeland Security in the Department.

Many of you will have heard about the Quadrennial Homeland Security Review. It was a review mandated by Congress and it asks us to look soup to nuts at everything that was required to make Homeland Security all that it could be as a Federal Department and indeed as a Federal and as a National enterprise.

So what does it mean we do? We think that primarily it requires, if we want to build a safe and secure, resilient place that we have to do five things and do five things well.

First, we have to prevent against another terrorism attack. This is job one for us. We cannot become complacent. There have been a number of things that we have been doing over the past 20 months that have been building on the efforts of the past seven years within the Department to create a resilient and a preparedness and a readiness if there were to be another terrorist attack, which we all obviously are working to prevent. And we are, can only be successful if everyone does their job, everyone has a vigilance, now everyone is prepared. We want to prevent and deter terrorists wherever they are and wherever they attempt to strike, not only Americans, but American interests. That is job one for the Department.

We have four other missions that we think are important as well.

Securing our borders, this means not only keeping out people and goods that might be dangerous, but also expediting legitimate trade and travel, to bring the economic vibrancy to this country that we know and that we especially need in these economic times.

The third thing we need to do is enforce our immigration laws. What does that mean? It means welcoming people who enrich our culture and our economy, again, while keeping out people who might be dangerous.

The fourth thing we want to do is ensure a secure cyber environment. This is a new mission. This is a national mission. This is a mission that permeates everything we do in the Department of Homeland Security. Cyberspace, cyber world really functions as, in my view, the very endoskeleton of modern life. It is a system that coexists with every other system that we know and functions today. It exists in many of the sectors that you represent here. And simply without a secure and resilient cyber environment, none of these other sectors will be equally secure and vibrant and we have called this out as a mission. It is important that we focus on this and that we understand what it takes to create a secure and safe cyber environment.

Fundamentally it means that we address two challenges; the challenges of securing our information and the challenges of securing our identities. Other than that, it is easy but that really is at the core and as a number of experts have said, including Jeff Moss, the founder of DEFCON and Black Hat, not one single thing we do in cyberspace today can be done securely. You cannot access the net, you cannot transmit, you cannot stop, you cannot shop, you cannot visit, you cannot do anything, confident that your information or your identity might not potentially be compromised. We have got to do more in fixing that and certainly we in the Department of Homeland Security recognize that we cannot do all that needs doing alone. The private sector is key here.

The fifth mission that we have called out as essential to creating a safe, secure, resilient place where the American way of life can thrive is the mission of creating a resilient nation, a resilient people, able to withstand all risks and hazards. Again, in DHS we have been building on the work that those who have come before us have done to consolidate that work, to understand best practices, and to build out, not only our

capabilities, but our understanding of what works best in each of these areas; preventing terrorism, securing our borders, enforcing our immigration laws, ensuring a safe and secure cyberspace, and building national resilience.

We also have a number of other responsibilities obviously that relate to our national security and our other interests but these are at the core of what it means to be in Homeland Security. It's the third largest department in the Federal Government but even at that size, we recognize that we cannot do all that needs doing. And here the partnership again is so important to us. So I encourage you in this forum to ask the right questions. Ask hard questions. What is the proper role of this partnership?; What is the proper role of DHS as we work together with you in building out more secure infrastructures across the various sectors that are represented here? Whether it is more regulation, I am not sure that it is but if so, where and how? Is it a more dynamic partnership? Is it multiple forums? What about the roles for State and local authorities and communities as well? How do they fit into the equation?

We have a number of ideas about where we think and how we think we can go forward. But again, we want to hear from you. So I thank you all for your commitment to Homeland Security. I thank you for your commitment to this partnership. And I look forward to hearing the results of what we expect to be a very fruitful conversation. Thank you very much.

TODD KEIL: Thank you, Madam Secretary. And it is also now my pleasure to introduce Clyde Miller, who is the private sector Co-Chair of today's event. Mr. Miller is the Chair of the Partnership for Critical Infrastructure Security, PCIS. And in that role, he represents the leadership of the CIKR Cross Sector Council. Mr. Miller has also been active in the partnership since its inception, as a member and Immediate Past Chair of the Chemical Sector Coordinating Council. Clyde, thank you for being here.

CLYDE MILLER: Thanks, Todd, and Deputy Secretary Lute, thank you for your comments.

JANE HOLL LUTE: Thank you.

CLYDE MILLER: The PCIS, the Cross Sector Coordinating Council exists to provide leadership and facilitating cross sector collaboration with the government, working across the sectors to identify interdependency risk and to improve outreach among the sectors and the government.

Some of the challenges that we see sectors frequently facing are the multiple requests for information and participation in projects and other initiatives being pursued by various organizations both within DHS and other sector specific agencies. We try to identify those duplicative efforts and frequently have been successful in seeing some of these efforts consolidated into more efficient projects.

When Secretary Napolitano came to DHS, it was clear that, as a former Governor, she would push for more collaboration and information sharing with State, local and tribal organizations. The Council however had already begun this initiative by inviting the State, Local, Tribal, and Territorial Government Coordinating Council to our quarterly meetings,

realizing that the linkage to the, to those government organizations was critical to a successful partnership framework. That effort has led to a number of collaborations, some of which you will hear about later in today's meeting.

Cyber is another area of focus for the Council and our members have been involved in a number of meaningful cyber related initiatives, well before cyber threats became such a well known issue.

Finally, interdependencies have become a major focus of the Council. The Nation's infrastructure as we all know is intertwined in a complex web of dependencies from our communications backbone to our electrical grid to our vast transportation sector. Our Council is unique in being able to reach across all these sectors and highlight the interdependencies. We have done a lot of work with our partners at the national level and now are moving to regionalize this effort.

One of the things to remember is that all of us on the Sector Council, Cross Sector Council have full time jobs, so our initiatives have to be carefully weighed to insure that we're putting our limited resources to solving valid and meaningful issues. Over the last year, we have participated in a series of critical infrastructure roundtables hosted by Secretary Napolitano that served to provide a forum for sectors to share concerns, offer solutions, and opportunities directly with the Secretary.

In one way or another, the Council has always participated in national level exercises but NLE 10 raised the bar and NLE 11 promises to show what an active or and true partnership can do for a successful, meaningful exercise. Through the efforts of Bob Dix, the Vice Chair of the Council, the private sector and NGO's have a seat at the table in planning for NLE 11 as well as participating in its execution next year.

And I mentioned the Cross Sector interdependencies earlier. Later, one of our panels will be dedicated to discussing this important effort that's been led by Ken Watson, the past Chair of our Council.

And last but not least has been our participation in cyber. Council members hold two of the three Co-Chair positions on the Cross Sector Cyber Working Group. Over the last year, they have been integrally involved in the follow-up efforts of the 60 Day Cyberspace Policy Review, the Cyber Incident Response Plan and the National Strategy for Trusted Identities in Cyber. And you'll be hearing more about that in one of our panels later as well.

Moving forward, the Council will be championing information sharing across sectors and down to the local level by leveraging our relationship with the State, Local, Tribal, and Territorial Government Coordinating Council, the Regional Consortium Coordinating Council, and the National Council of ISAC's. Our goal is to facilitate seamless sharing of information across all of our sectors.

Later you'll hear from two panels. One on interdependencies and one on cyber information sharing. When putting together today's agenda, the intent was to have these panels create discussion or generate discussion with the audience.

Please don't be shy about participating. We certainly welcome your participation. Thank you.

I'll now turn it over to Ulie Seal, who's the Fire Chief and Emergency Manager for the City of Bloomington, Minnesota and the Chair of the State, Local, Tribal, and Territorial Government Coordinating Council. After Ulie will be Mr. Tom Moran, the Executive Director for the All Hazards Consortium and Vice Chair of the Regional Consortium Coordinating Council. And then finally Will Pelgrin, Founder and Chair of the Multi State Information and Analysis Center and Chair of the National Council Of Information And Analysis Centers.

Ulie?

ULIE SEAL: Thank you and just because I have a hard time saying State, Local, Tribal, Territorial Government Coordinating Council, I am going to use SLTT as an abbreviation. Otherwise, I'm not going to get through this. Our mission really is to provide a means and enter in a partnership with DHS and CIKR owner-operators on the NIPP and its implementation. I mean, that's kind of it in a nutshell for us. And our primary functions are to communicate, coordinate, plan, share information with DHS, the SSA's, and our CIKR owners and operators.

Our key initiatives are really to facilitate the NIPP implementation at the SLTT level, integrate CIKR functions into local fusion centers, participate in the development of our Sector Specific Plans with our SSA's, aid in the development of regional partnerships and we've constituted a new working group to take that lead, collaborate with DHS on chemical security planning and information sharing, and collaborate with DHS on improving risk and asset management, and disseminating best practices and technical tools.

Some of our goals just for 2011 are; we're continuing to work with our Automated Critical Asset Management System or ACAMS, continuing to work with Chemical Facility Anti-Terrorism Standards or CFATS, and continuing to build what we call our alliance networks, and it's really a communication network for the SLTT to be able to communicate with our identified partners, including CIKR owner-operators, other State and locals, our DHS partners, our PSA's, and our Cross Sector Council partners, the NCI, the RC3, and which one am I forgetting? Clyde, you thought you were getting old. And our goals continuing are; to develop a information sharing systems that catalog and be able to push things out through our alliance networks, try to enhance our sector specific planning efforts with our SSA partners, continue to maintain and build our Council membership, there is that turnover that occurs in every Council and we're continuing to build that depth and breadth of representation across the country, and continue to communicate and participate with our NIPP Council partners and our CIKR Cross Sector partners, RC3, NIAC, the National Council of ISAC's.

Some of our accomplishments are listed, but the one I'm actually most pleased with this year is a much closer partnership and coordination with our IP partners, including the PSA's. And the primary reason I'm pleased with that is that communication and information sharing pathway and being able to provide that information back to our SLTT constituents that we're trying to represent. And that's all I got.

Tom?

TOM MORAN: Good morning, my name is Tom Moran. I serve as the Executive Director for the All Hazards Consortium. It's a non-profit formed by states of North Carolina through New York; nine jurisdictions as well as their urban areas. Just by way of background, I came up through the private sector in the telecom space with GTE and with Verizon and then the towers fell during 9/11, they fell into one of our facilities and I had a lot of friends affected by that and I went up there to help out and came back a different person. And I didn't know what critical or infrastructure protection meant, but I served, I volunteered some time to the State of Maryland and ended up getting involved in this small partnership in the national capital region, which evolved into a consortium. And then when the NIPP was turned up, there was a opportunity to serve again with this regional consortium of consortiums and that's what stood up the RC3.

So I'm honored to be here today. And once again, I'm impressed with the number of the people that would take time to help this important mission. The consortium's mission is really to help facilitate partnership. If you look at our mission statement, we were formed in 2008 to establish, to find existing regional entities and to foster their growth and connection to other regional entities. One of the most difficult things here is how do you know who's doing what? It's a very, it's a big issue across the country, not just in a small region. So that's the focus of the Regional Consortium Coordinating Council, to coordinate with the other councils, but also to reach out and find groups that are out there working on this important topic of critical infrastructure protection and interdependencies.

Next slide shows our map of our coverage. It's growing. This is an evolving process. It will list, you can't read them all there, but in the handouts you'll be able to see the different organizations. The white areas are still uncovered, but we're working hard to do that.

Next slide shows our Executive Committee. I know many of them are in the room. Matt Morrison is over here on the side and I think Ian Hay is here. I'm not sure, Ann Beauchesne. These folks have invested a lot of time and energy. To my knowledge no one's getting paid. So this is another volunteer army. And it's been a pleasure to work with them. All of them are running successful organizations on their own, but have come together to kind of help this effort within the RCCC or the RC3 as we call it.

Next slide talks about our membership. This was a tough conversation. We had a lot of conversations around this. But what ended up coming down was membership in the RCC, RC3 has some requirements. One, they just, the organization, it must be, have a mission for CIKR. It must be a public private entity. It must be addressing regional issues. And region can be defined as, you know, two counties or five counties in a state or two states or six states or eight states. Region is flexible with that regard, because these organizations form for various reasons. It could be a group of tribes working together. It could be a group of states. It could be five states working on pet evacuation. It could be a number of reasons why they stand up. There's no cookie cutter. But all of them have passionate individuals and a mission that we try to

link into what we're doing if it fits. They must be a viable existing organization.

DHS was very clear not to start up organizations. Things that tend to do that may not survive as turnover changes and things. So we were looking for organizations that were existing and viable, could stand on their own. And they were, needed to be a non-profit. This was a long discussion around this, but they should be incorporated as a legal entity and exist as a non-profit.

Next slide really is kind of the meat of the matter is the RC3 works very closely with the SLTT and the other CIKR Coordinating Councils. And our mission is to find that red area in the middle that what we can do to help facilitate. The RC3 has a tremendous network of non-profit organizations who have people, memberships, companies, that they can pull information in to support a mission or they can push information out to educate the public. It's really a phenomenal network of people and organizations out there. And so we're going to be, we've been talking over the last year of how we can find those areas we can help facilitate in the middle.

So, the next slide talks about our objectives. In a nutshell, outreach is one of our number one objectives. Just to find out who is out there and who's existing and what are they working on? What are their capabilities? We're also looking at a resiliency study. This is funded by DHS through their staff that supports the RC3. That will be looking at cataloging some of these organizations that are out there; what their capabilities are and who their members are; all to serve as a resource to you folks within your respective regions; to identify these partnerships and how they can be tapped.

We're also looking to develop a common attributes and capability catalog if we'll be able to do this. Why is this important? Well if you're wrestling with specific issues, you need people in that region that can help muster information, support, partnerships, and really push this down to the small businesses that may not understand their role in the CIKR mission. And it's very difficult. We were talking to several of them once and why should care about, you know, CIP? I run a bakery. Why is this important to me? And somebody said, well, when the trucks can't get to you to deliver your bread, your bakeries out of business. And how do you spell this CIKR thing again? I mean, you get their attention that way. But that's part of the education that I think has to happen to the millions of small businesses that really don't understand they have a very important role in this topic.

As a, next slide talks about our goal here is to organize workshops within specific regions. Last year, we met and said, what one thing could we do to help bring together local, regional efforts? And so this was a concept we drafted. When the report's finished, we'll kind of move in discussion on how we do this. But these will be done on a regional basis.

They would bring State, local, tribal folks together along with private sector on specific topics, facilitate those, come out with some common issues and drive out what one or two things can we do in this region that would be relevant to the private sector and government within that area?

And last slide talks about our goals. I think this is the people side of the effort. I see the RC3 as an important role in educating, grasping what's out there, serving as kind of a scan for who's doing what in a certain area. And the trouble is there is no one size fits all. Each region has its own threats, has its own resources. And there are common things across all regions. Like cyber security's one that goes across the board. So we, we're looking to kind of help custom tailor the discussion that meets with the state and the private sector needs and focus on small steps that can drive quick wins. When people see a result, they stay engaged. No result, the meeting kind of degrades to conference calls and then eventually it goes away. This is what I've noticed over my five years. So I'm very proud to be part of the RC3 and its organization. Working very closely with DHS and Renee.

Just let me recognize Renee publicly. She has put in yeoman's work on this, working across the specter, along with a lot of other people. So glad to be here and thank you again for organizing this.

WILL PELGRIN: Hi, good morning, I'm Will Pelgrin. I'm the Chair of the National Council of ISAC's. For those that may not know, an ISAC is an Information Sharing and Analysis Center. Its mission is to help defend, protect, respond to whether it's physical or cyber events whether man made or natural. It's predicated on a firm philosophy of collaboration and cooperation that the Deputy Secretary's so pointedly said this morning in her opening remarks.

As Clyde mentioned some of the challenges, let me sum up the challenge that I feel that we face as a country, we can talk about cyber events, we can talk about physical threats, it is speed. If you boil it all down, when you think about how fast everything is moving, how fast the technology is being developed. How fast is that technology being implemented? And how fast of those that may want to do us harm are taking advantage of some of those vulnerabilities that may be existing. So our job is to keep pace with that speed.

Some of the changes from last year when I presented is first and foremost is our name has changed. It used to be called the ISAC Council. That may seem like it's just a word change, but to us it was really very specific to our goals and our mission. In the past, the ISAC Council had very strict criteria as to who could be at the table. As the Deputy Secretary said, if we're not all at the table, we're not going to succeed. So within the last two years, including last year with the change of the name to the National Council of ISAC's, our goal was to ensure that we had every critical sector represented. Recognizing that there is a maturity level of different sectors relative to their ISAC capabilities. So I'm pleased to say that we've grown from 10 or 11 sectors being at the table to over 20 and growing still. Our goal is to go out and reach every critical sector that needs to be there. Some of the goals that we had in addition to increasing the membership around the table, we built a directorate.

The sole concept is how do we share information? Not as an end state of sharing, but that it's actionable, implementable. That we can actually make a change to improve our posture, whether it's from a physical perspective or a cyber perspective. Part of that information sharing is how timely can accurate information be shared? And part of that is how

easy can it be done? So we've created a digital dashboard or virtual op center.

All of the ISAC's have mapped their alert levels to a common alert level, so at any one time, if you went to that directed, you would be able to see where the multi site ISAC is, where the IT ISAC is, where the financial sector ISAC, and all the other ISAC's are as they relate, rate themselves from either a threat perspective or consequence perspective. This is still a work in progress. Not everyone is using it. It was just implemented during the year. But everybody sees the value of this.

So when a crisis is occurring, when you have think about does Will Pelgrin need to know this? You don't have to really think about it, because it's all on the dashboard. Secondly, it's critical that we continually have that relationship with the law enforcement community, and in particular, the fusion centers.

Our goal from a national council is to develop those relationships with the fusion centers, to understand what their responsibilities are, and more importantly, to understand what we can contribute to help them on a day to day basis from a situational awareness.

As I said, we have now a common alert level that we map to. It doesn't mean that our individual alert levels have changed. They haven't but they can be mapped to a common one. Those protocols are really critical.

There is a pilot on cross sector sharing that's going beyond just sharing of information after the fact. This is a group of ISAC's that came together to share real time data and to analyze that data from a cross sector perspective. Our goal is that is where we need to be as a country. We're working very closely with DHS on this as an integral partner.

I'm very pleased that we were involved in Cyber Storm III. DHS deserves a huge round of applause for a Herculean task to pull this international event off so successfully in our opinion. Even though it's not about how good you are in exercises, it's really about how good you can be in those lessons learned from that, so that can we improve upon our behavior and how we would respond if a real world incident occurred.

And lastly, I have to give a plug. This is Cyber Security Awareness Month. Tomorrow there is a national Web cast that we're hosting for free. Please go to our Web site at the National Council Web site, multi-state, any one of the Web sites should have it on it, DHS's. Four of the ISAC's are presenting, along with DHS. This is open to everybody. It's actually has right now I think four countries that are participating as participants in it and most of the states. It's a great opportunity to hear from the experts about what you can do to help protect yourselves, not only at work, but in the private sector, at home as well. With that, I'll stop.

CLYDE MILLER: The first roundtable is going to be on interdependencies and regionalization. It's going to be moderated by Ken Watson, the former Chair of the PCIS Cross Sector Coordinating Council, so I'll turn it over to Ken to introduce his panelists.

KEN WATSON: Thanks, Clyde. Interdependency is one of the Holy Grail issues of critical infrastructure protection and it has been for a long time. In my 12 years involved in this initiative, I've seen several national governments attempt to get their arms around it. Canada was first and it was a monumental effort that they put together, resulting in a wall sized chart of dependencies and what it showed was that every sector depended in some way on every other sector. The United States has made similar efforts with similar results.

Several National Level Exercises and actual events have demonstrated that there are dependencies that are unique at the local level. We go back to the TOPOFF 4 exercise, which illustrated the national dependence on Portland, Oregon and Phoenix, Arizona for the manufacture of radio isotopic medicines. That was brought to light by the nuclear sector, which participated in our PCIS simulations cell for that exercise.

Another illustration from that exercise was the interdependence of food and agriculture and how a motor carrier bringing perishable food across the border. If the Secretary of Homeland Security has declared Homeland Security Alert Level Orange, then you require inspections for everything. That may delay the passage of trucks across the border and jeopardize the availability of foods around the nation.

Hurricane Katrina and subsequent hurricanes demonstrated the interdependence of rail, chemical, water, and public health. Another example of this are the railroads having to devise a work-around to deliver chemicals for water purification when the rail beds were undermined in Louisiana.

These issues highlight to us that, yes, you can define things functionally at the national level, but you really can't get to actionable information unless you get down to the regional and local level. So PCIS launched an interdependency initiative a year and a half ago with the eventual purpose of developing and understanding of regional and local dependencies.

We started with a national level functional description of each of the sectors. We have had several sectors participate so far and we're not complete around all of the sectors.

Then, we had cross sector meetings to identify dependencies. We're planning to use those dependencies for scenarios to take to local workshops to bring business planners or business continuity planners together to work through those issues.

Today we have the draft interim report from that study and the next step is to use that to go to regional workshops as I said. We would like the local planners to do things to validate our methodology to make sure we have a repeatable process that can be taken around the country and then work through local dependencies to help bolster their resilience, which would raise the level of national resilience as well.

We designed the study from the beginning to partner with the SLTT and the RCCC organizations. We look forward to following through with regional workshops.

Each of the distinguished panelists we have on this particular panel has been involved in interdependency and regional work. I'll introduce each of them and ask them to spend a few minutes describing their most recent activities and some challenges that they're planning to face in the future. Then we'll open it up to a discussion with other CIPAC members in the audience.

Cherrie Black is an Assistant Attorney General in the State Of New Jersey and the Chief of Critical Infrastructure Protection Bureau in the New Jersey office of Homeland Security and Preparedness. In that capacity, she manages a staff of security specialists, preparedness planners, and project managers who coordinate local, state, and regional critical infrastructure protection and preparedness initiatives for the state. Cherrie is currently Vice Chair of the SLTTGCC as well as Chair of the SLTT's Regional Partnership Working Group.

Jeffrey Dell is Senior Vice President, Crisis Management Strategic Planning and Industry Engagement Team, Bank of America. Jeff has been with Bank of America for nine years. His responsibilities have included corporate security coordination to manage to the bank through planning, response, and recovery from any threat that may impact life, operations, production, and customers, both domestically and globally.

Matt Morrison is the CEO of the Pacific Northwest Economic Region or PNWER as it's more affectionately known. PNWER is a statutory, public and private partnership created by five states, three Canadian provinces, and two territories in 1991. PNWER established the Center for Regional Disaster Resilience soon after 9/11 to specifically address critical infrastructure interdependencies and design a nationally recognized Blue Cascade series of interdependency exercises in the Pacific Northwest. Blue Cascades have focused on both terrorist and natural catastrophic disasters and the resulting cascading impacts of critical infrastructure disruption in a five state international region. Matt has been CEO of PNWER since 1999 and is a founding board member of the Regional Coalition Coordinating Council or RCCC.

Finally, Don Robinson is Regional Director for the Southeast Region in the Department Of Homeland Security. Don has been with DHS for just under five years. In that capacity, he provides direction and focus to field deployed protective security advisors. His region includes Tennessee, Florida, Georgia, South Carolina and North Carolina.

And with that, I'd like to turn it over to Cherrie for her first remarks.

CHERRIE BLACK: Thanks, Ken. I'm going to make a reference to Matt Morrison in my early comments, because he's kind of a rock star of interdependency and he's going to be talking to you in a little while about the PNWER resilience tautology, which I'm going to just reference briefly here.

I'm going to talk about two New Jersey resiliency and interdependency related efforts that I think will demonstrate the validity of the tautology that Matt's going to mention. Both were multi-jurisdictional and regional. They looked at resiliency as a function of dependencies and interdependencies of critical infrastructure. Both supported catastrophic planning efforts that are going on in the state.

The first I'm going to talk about is the Exit 14 Regional Resiliency Assessment Program (RRAP) and my colleague at the end, Don Robinson, is going to talk to you a little bit more, in more detail about what a regional resiliency assessment plan actually is, but I'm going to reference what we did in New Jersey.

In 2009, the first year of the RRAP's, New Jersey received one of five or six RRAP's. The state was allowed to define the scope of the RRAP with DHS's advice and consent. We looked at the resiliency of five sectors within a 10 mile radius of Exit 14 of the New Jersey Turnpike. If you're familiar with that area, that's basically where the Newark Airport is and that area, that 10 mile radius, includes 70 percent of the nationally significant critical infrastructure in the State Of New Jersey.

We decided to look at five sectors principally, because they deliver mission critical functions that cut across all critical infrastructure sectors, and what we looked at were energy, water, communications, information technology and transportation. The key is that there are a number of key activities involved in an RRAP, but the one I want to focus on is something called a system recovery analysis, during which we brought together stakeholders from each of those sectors.

We brought in key public and private sector members to basically deconstruct what are the external critical needs of each of these sectors, systems, and assets and by external critical needs, we asked them to ask themselves: what are the requirements I don't control that affect my ability to remain operational? The reason we asked them to think about those things was because we're government. We're trying to figure out where government plugs into the whole interdependency equation.

One of the reasons we plug in is because we actually do control some of those external critical needs. Items that emerged included things like: supply chain issues, debris removal, access control, and the delivery of other lifeline sector functions to those critical infrastructure sectors.

So where are we with this? We made a start and the work continues. We are still working on the 2009 RRAP. An RRAP is not something that you just kind of start. One of the things we found out is that it has a defined end date.

We recently received a very detailed analysis of the Northern New Jersey water infrastructure from the National Infrastructure Simulation and Analysis Center. One of the things Matt's going to talk about it is the trusted relationship between the public and private sector and that's one of the examples of where that really comes in because we have six water systems in Northern New Jersey, each of which gave NISAC their master plans, their hydraulic models, and an interconnection

study that had been proposed and cooperated with by these private sector and public sector water authorities. That is unprecedented. I think it's a level of true data that NISAC has never seen before for a region in the country and it illustrates what you can do when you actually have that trusted relationship between the public and private sector.

The next thing that's going to happen with the Exit 14 RRAP is that a tabletop exercise will likely occur in the first quarter of 2011. New Jersey is using the funding from the RRAP to develop a decision support tool to support prioritization of resources and efforts in a post-disaster scenario.

The other thing I want to talk about real quickly is the Regional Catastrophic Preparedness Grant. Northern New Jersey and New York were both recipients of FEMA's Regional Catastrophic Preparedness Grant and I was the Project Manager of a Regional Infrastructure Protection Plan. I was allowed to define what I wanted to do with that plan with the advice and consent of our entire private and public sector constituents in New Jersey and we looked at essentially asking the question: what will the impacts be of a major long term disruption to the electrical sector?

We were thinking, initially, of impacts to other sectors, the usual cascading effects. However, the fundamental criticality of the electrical sector brought us back to a focus on the challenges and impediments to restoration of that critical function because virtually everything else depended on that: traffic lights, pumping water into buildings so toilets flush and faucets run, telecommunications, information technology systems, the ability to make our transportation system work.

We really did not focus at the end of the day on cascading impacts. We focused on the restoration, supply chain issues, and governance issues that will arise when there is a catastrophic disruption to a critical function like the ability to have power in a highly populated region such as the New York and New Jersey areas.

One of the ways we did that was through a series of three facilitated workshops that brought public and private sector stakeholders together. The first workshop really focused on the coordination of emergency response and short term restoration effects and the players included regional electric utilities, market operators, reliability coordinators, energy management, emergency management agencies, and other government agencies. They looked at the attempts to perform rapid restoration, looked at government response, public messaging and security fire suppression. What happens when the place that you need to do the restoration is suddenly a crime scene? All of those issues were looked at and discussed in after action reports.

In workshop number two, we looked at recovery and supply chain issues and, again, the focus was on the long term recovery and return of the power system to normal operations. The focus was on the transformer supply chain challenges with two, and we actually had two transformer manufacturers at the table to talk to us in very clear terms about supply chain issues, about logistics issues and about the movement of these assets from one place to another. We got the real ground truth on

what is actually available to replace multiple destroyed transformers at any given point in time. We also heard from some of the electrical groups, such as the Edison Institute and the PJM Spare Transformer Program, on how those scarce resources will be allocated.

The last workshop looked at governance issues and basically how government will react when we are asked to apply scarce resources across a given region where there are multiple competing demands for scarce resources.

Those are the two efforts that we have going on in New Jersey and I look forward to taking any questions on those.

KEN WATSON: Thanks.

JEFFREY DELL: First let me thank all of you for the honor to be here to speak to you all today. I'm here to discuss the really the thematic nucleus; the many themes that we're hearing: the interdependency, private-public partnership, intelligence sharing and education and what we think to be the thematic nucleus as it resides in our fusion center.

The Northern California Regional Intelligence Center is based in San Francisco, California. The NCRIC, as it's commonly referred to, is a cooperative federal, state, and local public safety effort to centralize the intake, analysis, fusion, synthesis and the appropriate dissemination of criminal and Homeland Security intelligence in the Greater San Francisco Bay Area and in the Northern Coastal Counties of California. It has its roots in the traditional law enforcement intelligence community, although it has evolved to include an all-hazards construct in all cross sectors and to include private-public partnership.

A couple of program highlights I'd like to share. Under the direction of Mr. Caverly, a private sector liaison officer was put in place, a gentleman named Brandon Bond. He established a primary point of contact for Critical Infrastructure and Key Resources, linking both the fusion center to the private sector. He started with outreach and identified, through various meetings and workshops and conferences, a core working group of private sector representatives from organizations large and small.

It seemed to me the common theme really was two-fold. First, the representatives he selected had authority around policy and experience in operations and tactical response for their organizations, but also had a very strong social responsibility mission within their respective organizations as well. That is the intent in the development of the fusion center. It wasn't solely for the benefit of our respective organizations, but for our regional community at large, including mid, small sized businesses, non-profits, and faith based groups. He wanted to create an intelligence center or fusion center that, at some point, helped all of those organizations to some form or fashion.

We met a number of times to identify the mission and to identify both the function and the utility of the fusion center and what it could provide us. It started with the very basics: intelligence support and sharing timely and actionable information. It also included suspicious activity reports in a bi-directional communication model.

In other words, we knew immediately that the benefit of a fusion center wasn't simply for the government to help us as private organizations, but that we had a mutual responsibility to share information multi-directionally, both to the government and to other organizations that could also be impacted by various threats or information that came to our attention.

The intelligence support to suspicious activity reports was a big piece of that process, in addition to the mechanism to report CIKR and local support, helping private companies understand what CIKR really means and how to identify and coordinate the assessment through ACAMS and specifically through special events, as they were coming up within our respective areas. Some of the specific program elements include the NCRIC distribution list. It sounds very simple, but it really was a critical piece of this process, in that really what we built was a network of networks and recognizing that the first distribution group really created the first control point within which information could be shared. Depending upon the classification of the information, the information could be disseminated out further to sub-distribution groups within the network.

The Alert Notification System was a very important piece of the program, along with weekly FOUO conference calls highlighting tips and leads as they're made available to both distribution center analysts and to us; also, classified, non-classified briefings and access to the Homeland Security Information Network. This turned out to be a critical piece of the process.

To operationalize our model, we needed a common operating area to share information and, again, in multiple directions. We were included in the development of the Homeland Security Information Network, the HSIN portal for the NCRIC. Christy Riccardi and her team flew out from Washington to San Francisco. A few of us sat down in a closed door session to brainstorm and white board and we identified the function and the utility and the aesthetics of a graphic user interface, including all the various links we felt necessary to deal with the business as usual or the day to day information and highlights of the intelligence community, but also at time of disaster. The development of a regional portal allowed us that secured and vetted control point for the string of information. That was one of the bigger challenges that we presently face and continue to today.

We understand as large organizations that we have both information and services that provide us, for example, meteorological forecasts. We have impact data around our facilities and our infrastructure and it's a cultural shift to be willing to share that kind of information in any forum outside of our organization. We sat down at a number of sessions, including a CIPAC conference in Santa Clara County not too long ago, and this became a topic of conversation. I will tell you that we're all steadfast in our willingness to work through the challenges and the HISN network and the fusion center really came into play during a real activation. This is no longer a theoretical model. It's actually been tested in a real world event during a large demonstration post trial in both Northern and Southern California.

What we discovered was three very important elements, successes truly. The first is that with the access to HISN and our relationship to the NCRIC and the fusion center, we were asked to provide intelligence around our posturing to prepare for the impact. We were asked to provide the closures of our buildings and the release of our associates, to the degree that we were willing to do it. We shared that information, uploading it into the HISN network and it was used by the incident command for the deployment of resources. We were receiving information from the intelligence community through the fusion center through the HISN portal. We were able to download updates, intelligence updates and tactical information, that we also used ourselves to further evolve our decision making through the evolution of that event. The third piece is through the California Resiliency Alliance, which is one of our network partners if you will, representing a much broader group within the State of California. It has seats in the emergency operation centers, both the regional operation center and the state operation center. Those folks sitting within EOCs were able to gather intelligence and situation reports and post it to the HISN network so that we could then cascade that information out to a larger, broader audience.

What we really have now is a closed loop. We have completed the triad. We have the Incident Command communicating through the fusion center, the private sector, communicating through the Emergency Operations Center, Atomic Disaster. We felt it's an exceptional model. We understand there are many fusion centers out there. We have our finger on the pulse of many of them. We're linked in every chance we can and share best practices across the board to further collaborate to build out these fusion centers to the greater success of the program. Thank you.

MATT MORRISON: I'm Matt Morrison, Executive Director of the Pacific Northwest Economic Region, which is a bit unusual. It is five states and five Canadian jurisdictions that were formed 20 years ago for the economy in the region and it's through the lens of economic security that I come to this table on critical infrastructure resilience. I think our effort began right after 9/11, looking at the interdependencies between critical infrastructures and how absolutely vital they are to our regional economy. Cherrie mentioned this.

I'm going to just share this from our experience, a resilience tautology. A resilient nation requires resilient infrastructures, assets, communities, and citizens. Resilient assets and infrastructures require resilient regions. Resiliency requires understanding which assets are critical in any specific scenario and understanding criticality depends on understanding the interdependencies between and among critical infrastructures. Here, the thing is that criticality is dynamic and changes hour by hour in any incident, so regionalism is really vital in understanding criticality on specific scenarios.

Understanding interdependencies requires 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. Trust is local. It's built by face to face interaction in a community where people know and depend on each other and public-private partnerships on a local and regional level are

necessary to build this trust, awareness, and shared sense of responsibility.

I think that this really encapsulates our efforts over 10 years at looking at cross sector coordination in a regional model. We have thousands of stakeholders that have been involved in workshops, seminars, tabletops, and action planning sessions. We have a regional disaster resilience action strategy that's the compilation of seven Blue Cascades Exercises and many, many in-depth meetings based on that trust.

You know, in the beginning, the private sector wanted everyone to sign a non-disclosure agreement for our tabletops. What was unique about our process was that it was, in a sense, owned and run by the private sector. It wasn't government saying, "well, we want to explore this scenario, will you come and join us?" It was a scenario designed, created, and built by the private sector, sharing among themselves their deepest concerns and what they wanted to explore and we've had Blue Cascades on terrorist attacks on the electrical grid and went to great lengths on those high voltage regulators. Cyber attacks, large abductions, an earthquake in the region, pandemics and how do critical infrastructures function in a pandemic situation, supply chain resilience. Flood scenario: we've, with the Dam and Levees sector, done a dam and levee exercise series in 2009 and 2010. Finally, our latest bio-event resilience: Community Resilience.

I think that what we've seen is that this trust is really critical and it takes a public-private partnership, a trusted convener to bring the public and private sector together. It is also necessary with the private sector never to have a meeting that doesn't have clear deliverables for the private sector. Government likes to call meetings all the time to ask for information. What I have seen over these nine or 10 years is that you cannot do this overnight and you really have to invest in conveners.

We have a very successful program. I think it's been recognized. Yet today, six months from now, I don't have any funding for this program. There is no mechanism to support the conveners out there and I think that the public demands that we do this kind of work. It is very clear to me that it is absolutely vital to our long term resilience and that, rather than just looking at a national level at what are the critical infrastructures, we have to look at communities. We have to look at regions, whether they may be metropolitan or multi-state. You have to have an elastic boundary when dealing with critical infrastructures.

When the government of Washington says, "what's the most critical infrastructure in my state," it might be a thousand miles away in another state and we've been able to, over time, educate the emergency management community, law enforcement, and the private sector on looking elasticity at these boundaries. Out of this process, we have developed, and we facilitate, a number of sector, regional sector councils in the region. Northwest Cyber Security Alliance and the business and or the banking and finance community. We have fostered state by state public-private partnerships to address their particular needs.

In all of these exercises and workshops, information sharing always rises to the top and we were able to go through a process of two years listening to the private sector for what they want out of a fusion center and developing a concept of operations that's actually being implemented now in the Washington State Fusion Center .We have 2200 vetted security professionals that are sharing with each other and the fusion center is able to observe that traffic and bring in subject matter experts in a moment into the fusion center. I think what is really vital, as we look at interdependencies and as we look at regional resilience (what the secretary talked about) is how this is a shared responsibility and that is really fostered by engaging the local businesses.

A lot of our funding has come from the private sector. They need to feel an ownership in the process and I really cannot emphasize that enough. I think that, by looking at how we foster these public-private partnerships, will go a long way to building regional and national resilience. The recognition of that criticality is that it may not be a big infrastructure. It might be something very small that like in a pandemic. It might be clean bed linen or a laundry facility or food and fuel, which are obvious. The more you explore what the local communities are concerned about, the greater the resilience.

I look forward to the discussion. Thank you.

DON ROBINSON: Thank you, Matt, and good morning, everyone.

As previously mentioned, my name is Don Robinson. I am the IP Regional Director for the Southeast. This morning, I am going to provide a brief overview of the Regional Resiliency Assessment Program, or what we refer to it as, the RRAP. The goal of the RRAP is to reduce the nation's vulnerability to all hazards by evaluating critical infrastructure at a regional level and coordinating protection efforts to enhance resiliency and the security of the surrounding communities and regions.

The RRAP is an interagency assessment of selected critical infrastructure. During the initial phases of the process, the Protective Security Advisors work very closely with state and local Homeland Security Advisors to identify or scope the area that we're going to look at. It is during these meetings that we identify the specific assets. Once the specific assets are identified, that information is sent to IP and IP conducts further analysis of those sites.

We want to make sure that we get as much input from the states as possible to determine that list because once we identify that list of critical infrastructure; we are going to begin the assessment phase of our RRAP. The RRAP examines vulnerabilities, threats, and potential consequences from all-hazards perspectives, using enhanced methodologies. Some of the methodologies that we use or survey tools that we use are the Enhanced Critical Infrastructure Protection Security Survey, the Site Assistance Visit, the Buffer Zone Protection Plan, and the Computer Based Assessment Tool.

The ECIP assists in identifying critical infrastructure interdependencies and resiliency characteristics and also identifies

gaps, using a methodology that identifies six weighted and scored categories. Those categories are physical security, security force, security management, information sharing, protective measures, and dependencies.

Another tool that we use throughout the entire RRAP process is the Buffer Zone Protection Plan. The BZP allows us to look at prevention and protection capabilities of local law enforcement, first responders, and owners and operators.

During the RRAP process, we also provide mitigation training through protective security coordination division. Some of the courses that we offer are a soft target awareness course, surveillance detection, improvised explosive device awareness workshops, private sector counterterrorism awareness workshops, and the protective measures course.

During FY09, we had a series of pilots. We had five pilots throughout the nation and I am going to briefly review each of those pilots. In Chicago, we did a financial district RRAP. In Tennessee, we did the Tennessee Valley Authority RRAP that focused on the Energy Sector. In North Carolina, we conducted North Carolina Research Triangle Area, focusing on the IT and Research Sectors. We also did Exit 14 New Jersey Turnpike Chemical Sector, which Cherrie talked about earlier. Finally, we did the New York State Bridges, focusing on the Transportation Sector for New York.

For FY10, we have six RRAP's lined up and we are currently in the process of conducting those assessments. Right now we have the Texas Pan Handle, which is in Amarillo, Texas and its focus is on the Food and Agriculture Sector. We did an RRAP in Atlanta, Georgia focusing on the Commercial Sector, Boston, focusing on the Energy Sector, West Virginia, focusing on the Energy and Chemical Sector, Las Vegas, focusing on the Commercial Sectors and Seattle, Washington, focusing on the Telecommunications Sectors.

Just a couple closing comments on the RRAP:

- As Cherrie mentioned, they are never-ending. Some of these started in early FY09 and we're still continuing through the process.
- The FY10 is still in process and all these RRAP's fall under the BZP program, which is a grant funded program that goes to the states.

KEN WATSON: Thanks, Don. Thanks, everybody. At this point, I would like to open it up to questions, first from the CIPAC members around all the tables and then we'll go to the audience. I have some hip-pocket questions, so we can keep the conversation rolling if no one wants to start. Please, who has the first question?

CLYDE MILLER: It is amazing how much work has been done out there in an effort to try to address the resiliency at the regional level and make these connections. In addition to these other things that I have talked about, as me being involved and also the Director of Security for BASF

corporation, we participated in a Buffer Zone Protection program up in the Detroit area a few years ago. We have a lot of concerns about providing the information that was needed to provide for that, because of the sensitivity of our facility up there and the danger or the concern about information getting out inadvertently as part of this process.

I guess I have two questions:

- Number one, how are you going about overcoming the resistance from your private sector partners and sharing a lot of detailed information about their weaknesses and about their vulnerabilities?
- And secondly, how do you go about or what kind of regime are you protecting this information under?

DON ROBINSON: I can address the first part. Actually, most of the information that we collect falls under the PCII program or the Enhanced Protected Critical Infrastructure Information program (ECIP) and our Buffer Zone Protection plans, our site assistance visits, our Regional Resiliency Assessment program surveys, the ECIP program. They all fall under that realm of the enhanced, or the PCII program. You cannot do these assessments without having good relationships at the state and local level and with the private sector and we actually have those relationships through the protective security advisors that are based in each state. They develop those relationships on a day to day basis with the Homeland Security Advisor and the owners and operators of the state that they live in. You have to continually massage that relationship and work at that relationship. You just cannot go in there one day and be demanding and request all that information, because you really have to understand the information that that owner-operator is sharing with you and you have to do your utmost to protect that information in every way possible.

BILL FLYNN: Clyde, if I could jump in there for a second just to echo Don's comments about the importance of that relationship, because it hasn't happened overnight. I think another important element about the progress that is being made here is that there is really true value to the private sector and to the owner-operator. In the early days, I think we collected a lot of information and we analyzed that information and we looked at how that helped us frame the risk environment, but we quickly learned that, unless there was value added, it was particularly working in a voluntary regime to the private sector, the open door policy, sharing information, discussing concerns, vulnerabilities, protective measures was going to be reticent. I think a growing element of the success of the effort has been both the trusted environment that we're working in and the protection that we can afford to the information, but I think that the feedback and the dashboards and the products that we can now provide to the private sector as a result of this effort is providing true value to them.

JEFFREY DELL: I would also like to add really from our point of view that there are two elements to working towards a solution and we are not there yet as an organization and as an intelligence and a fusion center, but we found that one of the key elements was education of our

organizational leadership and that they did not truly understand where the information was going, the value they had to the greater good and the protections that were in place. We discovered that, unfortunately, through trial and error as some of our assessors showed up at the front door of our critical buildings to begin the assessment process and our Presidents within those buildings were not aware of that process altogether, let alone the visit on that particular day.

The other piece that we are working really to overcome through the fusion center, which is not PCII protected, is the sharing of impact data at time of disaster. Do we really want to expose our critical infrastructure as it is currently being impacted by a hurricane, a fire, flood, or so forth? I think what we are discovering is that, the fusion center is not predicating the requirement of the sharing of the information or providing even guidelines for that matter, but allowing the private sector to find that common denominator of comfort. What are we willing to share, to what degree?

We know even through the HISN portal, which is the conduit for sharing that common operating area is secure through the (unintelligible) vetted process, there's still this network of network model. We want that information to be cascaded out through trusted networks, but we lose control at that point, and so what we are exploring now really is the provision of the information and to the degree we can scrub for any truly proprietary confidential data and then verifying that it is still meaningful and valuable when we upload it. It is a work in progress at this point.

CHERRIE BLACK: Clyde, just real briefly, on the RRAP, we too relied on PCIS and basically the trusted relationships that we built up with the asset owner-operators over a long period of years. It is a little bit different on the regional catastrophic planning grant effort. We instituted some information protection protocols for every activity we did.

For instance, probably the most sensitive information about the modeling that was done was revealed if at all at the first workshop we did, so we had tight controls over who participated in those workshops. Every electric utility knew who was going to be present from every other electric utility that was going to be present. We also, in the dissemination of materials to facilitate the workshop: we disseminated them, we numbered them, and we recollected them at the end of each workshop. The after action reports were all vetted by the participants and by each of the key stakeholders before they were finalized. We also had non-disclosure agreements for all of the players and most importantly, I think, we didn't ask questions that we did not need to know the answers to.

In other words, if we did not need to know something about what was going on inside the fence, we didn't ask that question and we did not try to collect information for the sake of being information collectors. What we were trying to do was figure out how government can support the industry in the aftermath of a major catastrophe so we only tried to limit our inquiry to those specific things.

KEN WATSON: Next question. Raise your hand. There you go. Robert.

ROBERT MAYER: Thank you. It is a question and part-comment. One of the organizations that I think would be very helpful to include in our partnership is the 50 plus public service commissions around the country. The public service commissions have very strong relationships with the telecommunications providers in their states, the electric providers, the water providers and, in some cases, transportation. They have a national organization called the National Association of Regulatory Utility Commissioners. Though, that organization has committees. They have an Electric Committee, a Telecom Committee and a Critical Infrastructure Committee and they also have regional associations that represent, for example, Mid-Atlantic states, Southeastern states. The question part is: to what extent have you engaged these state organizations?

I know in the communications sector, we're working to integrate them into our risk assessment, but I think there's a tremendous resource there because of their understanding on the ground of situations, their relationships with these sectors, and also their expertise. There are a lot of folks in these departments. I know, when I was in New York, we had an entire group focusing on just communications sector infrastructure. I would encourage us to start looking to them as a resource and maybe that's already begun. Thank you.

MATT MORRISON: We work closely with the Public Utility Commissions (PUC's). We called them and are doing a workshop with the National Association of Regulatory Utility Commissioners (NARUC) regionally, but they've been invited to a number of our tabletops. I think it is a great suggestion.

CHERRIE BLACK: In New Jersey, our Board of Public Utilities is our commission and they function as the sector specific agency for several of our sector working groups, including water, electric and gas and the telecommunications sector. They are involved and they were actually in fact engaged in the Regional Catastrophic exercise that we went through and, you're right, they're very helpful, very knowledgeable.

DON BROUSSARD: Thanks to the panelists. It was a very enlightening presentation. I found it very interesting about the RRAP. I have been involved in this security emergency planning business for several years and that's a new acronym I need to add to my acronym bingo list. I had a couple of questions:

- Is there an appropriate information sharing environment where we could learn the lessons of what you're actually learning through the process of the RRAPs to assist to other sectors? Like a water sector hasn't done an RRAP on a regional basis specifically for water. Is there a way that we could learn the lessons of what you're learning from RRAP?
- The second question is: is FEMA involved in the process? I know they are involved a lot in post-disaster, but are they involved in the planning exercises?

DON ROBINSON: I can answer the first part of your question first. FEMA is involved in some of the planning that takes place for the RRAP. We have very close relationships with the Federal Protective Officers that

are located at the regions and the RCCC's so, yes, they're aware that they take place.

As far as after action reports for RRAP processes, I know that they are completed. I am not sure to what protection level they are, but I know we do an after action report after each RRAP process.

KEN WATSON: Let me follow up with a more specific question for you then and maybe Bill Flynn. I know Don was asking about the releasability of that and if all the information is done, is collected under PCII, then it is not going to be releasable, but can we ask you to do what we have already asked the intelligence community to do: beef up your tear line process so that you can have a releasable, more generic version of general lessons learned that can be used by other sectors than the ones that you have assessed?

DON ROBINSON: Yes, I think the after action report's already in that format.

KEN WATSON: Can we get a link to a Web site so we can find that?

DON ROBINSON: I'd have to follow up with you.

MATT MORRISON: All our lessons learned are on RegionalResilience.org and it is quite extensive.

KEN WATSON: Next question. Oh, I see a card up. Vijay, identify yourself.

VIJAY NILEKANI: Vijay Nilekani, Nuclear Sector. My question for the panel is did any of your scenarios and or RRAP's or tabletops include the physical evacuation of people? During link-ins or WMD attacks or currently the sludge leak in Hungary, it's in all the moving of people and did you factor that in? It does bring in several of the sectors into play.

CHERRIE BLACK: Vijay, the two efforts that I referenced did not specifically deal with that. If we had spun the scenario out a little more and really looked a little more closely at what would happen in New York City as a result of the inability to move water, we would have definitely had to look at that, but I will say that there are a number of efforts that are ongoing in New Jersey to look at evacuation and the movement of people following coastal flooding or in anticipation of a hurricane, things like that, that are ongoing all the time.

JEFFREY DELL: Through the Northern California Regional Intelligence Center, we actually did manage or monitor, actually both, the movement of evacuation of folks through the Southern California wildfires last year. We were very carefully monitoring the zip codes that were impacted, both that were already under evacuation order and those under warning and we were posting those updates through the EOC up to the HISN network through the fusion center. Also, we were receiving or pushing out through the fusion center, through HISN, requests for resources from the private sector, cots, a thousand pair of underwear, assorted sizes for firefighters. The private sector each respectively stepped up and lent a hand where they could, so it became a really kind of a unique model in that respect. The first time we'd ever tried that

before. We had GIS mapping posted and it really helped us quite a bit as not just as the fusion center community, but as a private organization to help manage the dislocation of our associates and our executives.

MATT MORRISON: We have also done that, but our private sector partners are more interested in long term recovery, because that's where the emergency management goes home and they're three to six months out. How do we get in, restore our infrastructures, and in what order and how do we get a regional governance structure to make those vital decisions? That's a key element.

KEN WATSON: Boyd.

BOYD STEPHENSON: Boyd Stephenson, Highway Motor Carrier Sector. I just wanted to discuss, because it is our sector that is involved in the movement of people out of these areas, that one of the issues our colleagues that operate buses have raised in the past that comes back to a larger issue in all-hazards management is access control, particularly in the case of Hurricane Katrina, where we saw a lot of buses that were asked to move folks from the Super Dome out to disaster areas. Then, when they came back, they couldn't actually get into the areas around New Orleans, because they were stopped, to bring more people out. I want to suggest that it's not just the physical aspect of moving people out, because the private sector is actually quite good at that, but a lot of it is just the ability to get on the ground and to do what the transportation industry is best at doing, which is moving people and freight.

KEN WATSON: Mike.

MIKE ECHOLS: Mike Echols, Communications Sector. I heard you say that there was a RRAP for communications in the Seattle area. We're currently conducting a national sector risk assessment and one of our goals is to connect regionally and at the state level to make sure that we represent the country as a whole. When you performed this RRAP, what was the end briefing? Who are you connected with in the Communications Sector? We want to make sure that we're able to incorporate whatever results you got into our national risk assessment.

DON ROBINSON: The end result is actually a delivery of a few products to the state and to the owners and operators. We deliver an integrated protective measures analysis product to the state for their consumption to read and understand the dependencies, the interdependencies, and the cascading effects within the infrastructure that was looked at. That product is a PCII document and it's delivered to the state for their review. I'm not sure the specific process to provide that information to you, but we can coordinate that through PSCD locally.

KEN WATSON: For interdependencies, how do you build enough trust to get them to talk to somebody outside the world that they know for either the fusion center or other organizations and, from Don's perspective, how do you convince somebody this is not just another "we're from the government, and we're here to help," but to make it value-added for the private sector folks that you're talking to?

MATT MORRISON: A great question, from our experience, the scenario design team that we pull together to look at what are the greatest concerns becomes the most valuable. Usually it is thirty to forty people and they spend a lot of time hashing through "what about this" or "what about that" and I think that's where the kind of the trust begins. In this scenario design team looking at what are your biggest concerns and learning about infrastructures that they may not have realized can impact them. We always do a seminar or workshop and then a table top and explore these interdependencies. I think, again, it's a process over time of people getting to know other individuals that they really need to know, and building that trust.

DON ROBINSON: The value added part is huge when it comes to dealing with the private sector. From a PSA's perspective, when we do the enhanced critical infrastructure protection security survey, or the site assistance visit, or the buffer zone protection plan, we're able to deliver back to the owner/operator an interactive dashboard that the security manager can use as a tool to do comparative analysis of his facility to other like-assets within the same sector, so there is a deliverable there. There is something that is useful to him to use for his security processes. That plays a big role in enabling us to get over the hurdle of "I'm from the government, and I'm here to help." The additional part of that is just being there within that area and seeing that person and participating in a lot of the committees and the sub-committees throughout the year.

JEFF DELL: I think a part of it is leading by example. I think large organizations in the private sector, as well as the government can suggest and support the need for information sharing vulnerability and interdependency documentation identification, but until someone steps forward and is willing to actually do it, and open that kimono first, there's always going to be that hesitance. I think I've learned quite a bit, not just from our own organizational perspective, but through a trusted broker facilitating workshops, where we're coming through that front door, checking our egos and are able to simply share the criticality of some of what we think to be our critical infrastructures, only to discover that what we think is critical to the local environment and to the region really is second or tertiary in the prioritization scheme given what we learned from our partners at the table.

I would have not considered a pharmaceutical company's ten year-long standing laboratory study on the verge of curing a particular type of cancer as a higher priority to power than our data center, but that is a consideration. I would have never considered the various nursing homes in the requirement of power to their life support systems. More likely I would have thought traditionally the hospitals. And so, until we are able to gather in a trusted forum with a trusted broker, and so openly sharing, I don't think we'll ever get there. I think that's the first step in the process and I want to thank some of the folks at this table for facilitating those conversations.

KEN WATSON: The audience, if you could, if you have a question, please step to a microphone and I'll recognize you immediately. Otherwise I'll press on with my own. Oh, I'm sorry, there's one there. I didn't see your card.

SUSAN MONTEVERDE: Thanks, Susan Monteverde representing the Maritime Sector. Some of the lessons we learned from Katrina were that, for ports, three critical things were missing.

- First was electricity. That was very important and I think it's a real question mark for ports of who gets their electricity back first.
- The second issue is fuel. Some of the ports have actually decided "well, I'll just have a generator," but the generator needs fuel and what we learned in Katrina is the federal government was controlling who got the fuel in many cases and it wasn't the port.
- The third one, and perhaps the most important one, was work force. Work force didn't have housing, so, how do we insure the housing side of it for the work force to come back to work?

The question I have is how would those of us in different sectors tap into these regional activities? How do we know about them? How can we let our guys know locally how to get involved if they want to?

I don't quite understand the RRAP, to be honest with you. It's a new acronym for me. I know you quickly said what it is, but I don't really understand it, so maybe you could take a second and explain that more. How can ports get involved, if they want to? They might not want to because there's a lot of planning already done by the Coast Guard and locally on port security and I'm not sure they need to feed into these, but some of the interdependencies like electricity and fuel and things like that might be things they're interested in.

MATT MORRISON: Great point, and certainly the ports have been very involved in our table tops. Some of our table tops have involved 350 people for two days and we have the military, the ports, everyone involved in learning, but I think your question points out the need for the RCCC and we do have a website.

I think what we want to do is encourage people to connect with the regional consortiums that are out doing these projects and I think, after we saw Katrina, the stakeholders said our Katrina is a subduction zone earthquake that covers the entire Pacific northwest and would put us out of business for months, and that was a huge focus for us. We're looking at all of those issues and using the waterways as the resilient transportation quarter.

SUSAN MONTEVERDE: RCCC has a website we can all access?

MATT MORRISON: Yes, it is www.R-CCC.org, three C's.

KEN WATSON: You raise an issue about awareness, and that's been something that all of us need to do a better job of. We've heard from folks that "oh, this is all government work, and the private sector isn't doing anything." Well, you've heard from several of the panelists and by the dedication of the people around this, these tables, that there's a lot going on in the private sector, but all of

us need to do a better job of making stakeholders at the national and the local level more aware of what we're doing and how they can engage.

Thanks for the questions.

TODD KEIL: This may be a little late, but be sure and speak up. We have the advantage of having the speakers right behind us. As I came in just a minute ago from the back of the room, it's not projecting all the way.

JEFF DELL: I'd like to take a moment to plug the Homeland Security Exercise Evaluation Program and the website. I know it may be rudimentary for me to the folks here, but plugging into that site and that national process, there's a calendar that identifies every exercise going on in the country, from fire extinguisher tests in a local jurisdiction to county exercises to the states. Arizona has got a test coming up here November to NLE '11. You don't necessarily have to participate in person, but dialing into some of these, recognizing some of the associations, the policy groups that are associated with these exercises really is an eye-opener, demonstrating where the rubber truly hits the road with regard to some of the policies and the procedures that come out of these groups.

KEN WATSON: Thanks, Jeff. Let's take some questions from the audience. I saw someone try to stand up and we cut you off. Try again and please identify yourself. Thanks.

SUSAN MOORE: Hi, my name is Susan Moore and actually this is a question regarding awareness, which you all began to discuss just now. I'm involved in the Communications Government Coordinating Council and helped launch the Telecom and Energy Working Group to examine interdependencies between those two sectors. In our working group studies, the studies indicate that there are important analyses, assessments, pilots, and exercises underway in both sectors to determine and to address interdependencies. So the question is this: What is being done to capture and make accessible information regarding these activities in order to allow us all to leverage resources and to minimize any redundancies so that we can all insure that our resources are being used to take us to the next level, rather than repeat activities that may have already been completed? Thank you.

KEN WATSON: I might just redirect that over to the Communications Sector, GCC, and SCC.

ROBERT MAYER: The answer is not enough and I think you're spot on, because we find ourselves, as a sector, often being asked questions that have been dealt with in numerous partnership venues across the government. I do think there needs to be some repository so that we are able to very quickly make that determination.

MICHAEL ECHOLS: One of the things that we've done because of this issue is we're re-configuring our HSIN site to make it more useable for our constituents and we're building a repository of long-term power outage issues and people who are working on those particular activities that will help us to mitigate that issue. We're working with the Electrical Sector, Department of Energy.

CHERRIE BLACK: One response I have is that if a lot of our stakeholders on the private sector side thought that some of the analysis that we conducted in order to get us to the end state where we knew a little bit more about interdependencies were actually going to be revealed to the rest of the world in some kind of document, we would have far less willingness on their part to come to the table. Still, I recognize that there are lessons to be distilled from all of these activities and I think there's a way of doing that that communicates lessons learned and overarching principles without disclosing vulnerabilities or risk in a particular region.

One of the things that I just said to Ken a few minutes ago, it's kind of the same thing we just talked about in terms of there being a way to encapsulate what happens in an RRAP without revealing more than you want to reveal about a region's particular vulnerability. Maybe there is some kind of tear line document that could be shared and disseminated more broadly about all of these kinds of efforts, but it needs to be some kind of a communicated protocol.

JEFF DELL: We, in our infancy, have attempted to leverage the portal as a portion of the functionality to post bulletins. We, as private organizations, as members of the NICRIC, can post our exercise scenarios for sharing for use by other organizations. Some lessons learned, specifically, if they lead to interdependencies so that our partners within the fusion center can better understand what we would rely upon them for at times of disaster. I'll grant that it's in its preliminary stages, but that's the track we're hoping to go down in further model.

KEN WATSON: Okay. If I don't see you with a microphone, then I'll press on with my own questions.

HAL DALSON: Hal Dalson, Dams Sector. I've heard you reference the HSIN portal as an avenue for sharing some of the information. How does that tie in with the ISACs that are currently in use by some of the sectors such as water and electricity? Is there a tie-in between those two portals yet? Has it been thought of? Is this something that we're setting a goal for?

WILL PELGRIN: Will Pelgrin from The National Council of ISACs. It's been discussed frequently. The ISACS, some of them have access to the HSIN portal. I have access to it but not everyone has taken advantage of that. An issue is the interrelationship between the U.S. CERT portal and the HSIN portal is something that's been common conversation for awhile and a DHS representative can speak to this better than I can. I believe the goal is ultimately to have that integrated so that it's a common platform and much more easily to transverse back and forth between the two of them.

JEFF DELL: I did learn just last week that the NICC leverages to the HSIN portal to upload intelligence from the fusion centers so, as the NICC creates its situation reports, and cascades them out, it's taking a look at the HSIN network, which was new. We didn't know that until last week. We went on a tour and they showed us how this whole thing works and the organizational chart and we're pretty pleased to hear

that. Back to the point of education of our leadership, my manager happened to be in the room, and that further supported my momentum to continue to share information to the HSIN portal, as this awareness continues to grow to the value of it.

KEN WATSON: Don?

DON BROUSSARD: Don Broussard, Water Sector. Just in following up on that previous discussion, we've, in the water sector, reached out to DHS and asked them to make a pass through from our water ISAC so we don't have to have separate credentials and that's actually a work in progress. I wish I could announce it has been successful, but we're about a third of the way through that process.

WILL PELGRIN: Actually, for most of the panel, the question is, as you do your analysis and, whether it's from the state of New Jersey, or when you're looking at it across state lines, if you look at human assets as well as physical assets, we had a situation in New York when there was a major ice storm, and I was at the time the Chief Technology Officer and had every generator plotted and knew exactly where they were and could be deployed. What I didn't know was where were any of the people who could put them in? We learned that very quickly that you had to have that asset as well. The second point is, do you also look at interdependencies or the reliance on common assets that may be outside of one jurisdiction?

MATT MORRISON: That's a very, very good point. Certainly, we have really focused in on the human asset, especially in our exercise on pandemics, where everyone is hit at the same time and how do critical infrastructures continue to function.

The other issue you mentioned that's come up in almost every interdependency exercise we've had, whether it's the banking sector, they all rely on the same trucks to get cash out to the cash machines, or security officials in any incident, everyone draws from the same pool. That's another reason why it's good to pull together all sectors to be looking community-wide at resilience because, if you're just doing your own exercise, everybody does their own exercises on their infrastructure, but it's pulling them all together and those things emerge right away. That's a great point. Thank you.

KEN WATSON: I think it is Levees, but I can't see that far.

SUSAN GILSON: It is, Susan Gilson with The National Association of Flood And Storm Water Management Agencies and the Levee Sector. I wanted to raise this as an invitation to Matt and to Don. I actually serve on The National Committee On Levee Safety, and we are going out with stakeholder workshops and listening to your presentation and the issues with interdependencies and the economic issues, it seems like it would be very helpful to those discussions as well. We are meeting in Portland on November 9, and I just wanted to reach out to Matt to see if it's the type of thing where you may be able to help us reach out to some of your folks and the private sector and also to Don, because we'll be in Augusta in December. I'm not sure of the dates, but I'd be happy to send you some more information if I can get your contact info, but would that be the kind of thing that you think that you may be able to help with in terms of communications and input?

KEN WATSON: All right, I'll take a stab at it. Who pays for all this? Matt, you were talking about six months from now; you don't know where your funding is come from. Cherrie, you talked about a couple of grants that you accessed. How much of its private money, how much of its public money and what public money comes with strings? Can you talk, too, about the financing of all of these things?

MATT MORRISON: First of all, our larger organization is supported by the states and the private sector. The Center for Disaster Resilience has been funded by one off-pilot projects, where we've tried to get an inspired DHS leader to say "use us as a test bed." The last project was S&T. We did a comprehensive community bio-event resilience plan for the nation, looking at how we responded to H1N1 and so on and in the aftermath of a large anthrax workshop that was also going on in Seattle, but that was SNT Office of Health Affairs. The NCSF funded two of our Blue Cascades exercises. The Department of the Navy funded one, recognizing that they depended so much on outside-of-the-fence critical infrastructures, but there hasn't been a place to go to try to say this isn't a lot of money. We're talking two hundred thousand dollars a year for probably seven or eight events in the course of a year with thousands of stakeholders. The states and the local governments next week have our fourth annual interdependency forum that's sponsored by Seattle and King County. There's also some institutional barriers: when you have a public/private partnership that need to be looked at in terms of encouraging the private sector to be able to match federal dollars, which I think you'd like, but sometimes on the ground floor, there's mechanisms that aren't there to make that easy.

CHERRIE BLACK: Boy, that's true. We, in New Jersey, what we do, I have the privilege of working for the State Administrative Agent for Homeland Security grants, so I know what's coming in, and I know where it's going and I have a familiarity with the grant programs and the parameters of the grant programs. What a Critical Infrastructure Protection Manger working in a small state like New Jersey has to be able to do is envision ways in which we can get done these things that we think need to be done within the parameters of some of these grant programs. In New Jersey, we're fortunate enough to have an urban area security initiative region, which is nicely funded by The Department of Homeland Security and that's the area that happens to contain sixty percent of our critical infrastructure in the state so there's a lot of money in tier one Urban Area Security Initiative (UASI). I direct this to the private sector. If you happen to be situated in a tier one UASI area, you need to know your state administrative agency, know the people in your Homeland Security office, know who's making decisions in the region, and bring them credible, workable projects, or bring them suggestions. Find somebody in that region that you can work with that has the same interest in doing what you want to do.

You know, the one program I described in depth was the regional catastrophic preparedness grant. That's a FEMA grant. It goes out to certain metropolitan statistical areas and New Jersey and New York happen to be one of them. I think it goes out to nine or ten areas throughout the country. As far as I know, we're the only RCPG grant recipient that did a regional infrastructure protection plan that

focused on interdependencies and resiliency, but any one of the others could do it. It's just a matter of envisioning it and acting on it.

JEFF DELL: The fusion center, it's DHS, but also in combination with legacy funding from joint and task force and high intensity drug trafficking groups and so forth. The private sector contributes directly through time and challenge, putting a number of hours into weekends and evenings and so forth in lending a hand, but really, we contribute directly to associations within the region. Those associations, for example, California Resiliency Alliance, formerly Business Executives for National Security (BENS), Building Owners and Managers Association International (BOMA), and other groups that we sponsor directly through association membership dues, have members that link into the fusion center, both primaries and proxies and they're able to push information into the model, into the fusion center intelligence machine, if you will, but also then take information that cascaded out to a much larger, broader audience, an audience that we couldn't communicate with directly or indirectly, even if we tried. We reach down in that case to BOMA to a singular facility level and so, we're able to go from the federal level through the fusion center through associations down into that singular facility level and that's done again through direct funding through membership association dues.

KEN WATSON: Erin, you'll have the last question.

ERIN MULLEN: Erin Mullen with the Health Care Sector. I really just more had a reaction to Cherrie's comment. Cherrie, you know, I think the work you're doing in New Jersey is outstanding, but I did want to point out that while DHS and FEMA has done a pretty good job in localizing their grant programs all through FEMA, DHS isn't the only SSA and there are a number of initiatives that are occurring outside of DHS that don't necessarily get tied into and any number of other initiatives as well. And so, sometimes it's rather difficult to tie into all of the various different agencies that the private sector may interact with. I just wanted to make that point. Thank you.

KEN WATSON: That's a good point. Thank you and I'll turn it back over to the chair.

CLYDE MILLER: Thank you very much, everybody.

TODD KEIL: Let's give our panelists a hand.

CLYDE MILLER: Okay. I've got 10:45. We'll go into a fifteen-minute break and we will start back at promptly at 11:00 with our next panel.

BREAK - 15 MINUTES

CLYDE MILLER: Okay, I think so far we've had a great first panel and I will now kick off the second round table, which is going to be on information sharing and cyber security. Moderating the panel for us today is Sue Reingold, she's the Deputy Program Manager for the Information Sharing Environment of DHS and Sue, I'm sorry if I screwed that up. I messed it up for the Deputy Secretary a while ago, so I'll just let you tell us who you really are. But go ahead Sue.

SUE REINGOLD: Thank you and good morning everyone. Actually I'm the former acting Program Manager for the Information Sharing Environment, as well as the Deputy Program Manager for the last five years.

What we wanted to do this morning, as we move into the second discussion, is really talk about both the accomplishments and continuing challenges in sharing, collaboration and to access the information that supports the security of cyber infrastructure, and Deputy Secretary Lute talked about some of the strategic emphasis.

Just to kind of lay the groundwork, and I know many of you have probably looked at the President's Homeland Security strategy, but it very specifically calls for insuring a secure global digital information and communication infrastructure. One of the things that it does from a national policy perspective, of course, is recognize the importance of strong leadership and partnerships to effect changes in policy, technology, education and perhaps even taking a look at the law to ensure a more secure and resilient digital infrastructure. The Deputy Secretary talked about the challenges of securing information and securing our identities. So there's been a lot of attention too, to this issue, and we'll talk about it from both a strategic and a hands-on, operational perspective.

Just a couple of things I thought I'd point out. There's continuing to be recognition, for some time, about the importance of strong, public and private partnerships, being critical to enhancing the sharing of cyber threat, and vulnerability information. There was actually a GAO, General Accountability Office, report from this past July that summed up, I think, pretty well the continuing challenge highlighting that there are both private and public sector expectations about the exchange of useful, timely and actionable cyber threat information and alerts, and their point was that these expectations really need to be consistently met by everyone involved. I think that's part of the ongoing conversation about how do we make sure that we understand, from a government and a private sector and infrastructure sector perspective, what all of our roles and responsibilities are.

Finally, something interesting for those of you that may have been following the intelligence authorization, a bill that was actually passed, first time in six years, there's actually a focus in there on cyber security. There is, one of the many things, that are in there, a requirement that actually asks for within a year, maybe it was 180 days, a joint report from both the DHS and the Intelligence Community Inspector Generals, from both of them, that would be submitted to the President and Congress that actually describes how cyber threat information and intelligence is shared among the government and with those responsible for critical infrastructure. A very important point, the report is supposed to assess the effectiveness of said sharing.

What we'll try to do for you this morning, as I'm pleased to be able to turn to this great panel of experts here, who are really experienced hands in this whole issue of cyber security and information sharing. And as I said, we'll give you kind of that perspective from the strategic all the way down to the operational.

So let me introduce the panelists, and you've got full bios so I'm just going to let you know who's here. I'm going to start with Admiral

Michael Brown, the Deputy Assistant Secretary for Cyber Security and Communications in the National Program, Protection and Programs Directorate at the Department of Homeland Security. Obviously, he plays the leading role of the strategic perspective. He also, like many people on this panel, wear a number of different hats, but he also has a dual hat as a Cyber Coordinator for the Office of the Director of National Intelligence as national cyber responsibilities.

Following Admiral Brown is going to be Guy Copeland, who's here as the Co-Chair of the Cross-Sector Cyber Security Working Group. In addition, he's Vice President for Information Infrastructure Advisory Programs, but wearing the hat, he led the formation and serves as one of the Co-Chairs of the Cross-Sector Cyber Security Working Group, and he'll be talking about significant activities of the group and where things are going.

We'll hear from Bill Flynn, the Deputy Assistant Secretary for Infrastructure Protection at the Department of Homeland Security, who again, from a coordinated national perspective, will talk about what DHS is doing and then also, give more specifics about some programs and getting down to the operational perspective, as well.

Then we will hear from Will Pelgrin, who you heard from a little this morning already, wearing his hat as Chair of the National Council of Information Sharing and Analysis Centers, and in addition to, of doing that he setup the multi-state ISAC. We go back many years when Will did that. He's also President and Chief Executive Officer of the Center For Internet Security.

So, a panel full of many experts and we'll follow the same format that Ken and the first panel did, where we'll hear from each of the panelists and then open it up to CIPAC members for questions, and such, and then the audience.

So, Admiral Brown?

ADMIRAL MICHAEL BROWN: Good morning everybody. I thank you Sue. It's a pleasure being here. It's good to be the first speaker, being from Boston and being a Red Sox fan, and seeing I have a couple of Yankees fans that are going to follow behind me, I need to get my remarks in first, since my team's on vacation.

It is National Cyber Security Awareness month. It's a great time to be talking about what we're doing, and how it's a shared responsibility, and that's why it's so great to be here to see so many of the partners that we work with. I want to say that it's really not just a partnership. What I have seen, what I feel and live, is again, going back to the baseball analogy, it's about teammates. From where I come from it's about shipmates and that's what I see. It's not just the partnership, it's active engagement that we have had with respect to many of the things that we have done, and that we're going to continue to do.

I wanted to talk about some of those. We realize that there are lots of challenges, but also wanted to make sure that we recognize the opportunities and successes that we've had and continue to leverage and to build off of that. I think that it's critically important for where

we are to give some significant examples. We've done a lot of pilots, going to the information sharing, and the partnership that we've had. Whether it's with the state and local governments, whether it's with particular sectors on down, we're continuing to do that. What I have told our folks is pilots are good, but processes, capability, capacity, effectiveness and efficiency is better. Learn from the pilots, build on that. We can multiply each pilot by the number of potential partners that could be applied to that and duplicate it. We need to come up with the structure and the capability to leverage the things that we've learned, to leverage the processes that we've overcome, to understand where in fact there are hurdles. Some of them are, sometimes, significant hurdles and try to attack those to put them behind us, and that's what I see us continuing to do.

What we've done just recently, many of you active participants in the development, the strategy, the execution and now the after effect of the Cyber Storm III, the National Cyber Institute Response Plan, the National Cyber Security and Communications Integration Center. All of those things were put together just two weeks ago, and we saw the potential, we saw some of the effectiveness that can take place building off the information sharing and the partnership. I can't tell you what a difference it makes to be able to walk onto an operational floor and to be able to see the partners there, to be able to see decisions being made that are based upon information and operational tempo that includes both the private sector, the public sector, all of the partners that needed to be there.

I don't want you to think that it was perfect. That's why it's called an exercise. There are things that we knew before we started that were going to be lessons learned. We knew that there were things that needed to be done. We also needed to stress the National Cyber Institute Response Plan. And so again, that that vision and the act of participation that we had from you all and your partners is what's going to make our ability to operate in the environment where cyber is critically important and all the more operationally viable. So we're looking forward to continuing that.

To give examples of some of the hurdles, some of you are well aware that we've been struggling to get the right number of folks cleared so that we can operate at the appropriate level. But again, the exercise proved the vision and the concept. To be able to have secure operational decision making processes in place with the combination of the sectors and state and local governments with federal departments and agencies is just an enormous step forward. I need to continue to build up behind that and we will, and I ask for your continued active participation. We will continue to work on the incident and response plan and have several taskings including the couple of legislative actions that we need to make sure that we are working on. Again, part of what we have seen is the dialogue in the demand signal, we ask for that all the time. Give me the demand signal so that I can understand where we need to go in an operational venue forward, and I ask that you continue to do that.

I'll stop my remarks here, because I do look forward to the questions, and not just the questions, but the recommendations and where we should be going with respect to where we are right now on cyber security,

where we are with respect to the partnership, and how we're going to operate from a steady state into a significant incident.

SUE REINGOLD: Thank you, why don't we go to Bill Flynn to also continue from a DHS perspective.

BILL FLYNN: You caught me by surprise. Thank you, Sue. Good morning, as we've heard, I think throughout the morning's effort, that the flow of accurate, timely, relevant information and intelligence, regarding both threats and all hazards, is absolutely critical to protecting infrastructure. I view that both from a physical and a cyber perspective, both kinetically and cyber.

We've worked very closely, particularly the past year with our brethren in CS&C in the linkage between physical and cyber security. You heard earlier about our program. I'll go into a little more detail on that. Our cyber brethren are part of that effort. They have built in those cyber questions into our tool. We have done 50 joint assessments with them in the field. They are part of every major special event that we exercise and conduct our assessments with, so there's a real growing marriage there between the physical and cyber side of the house.

I'd like to talk to you a little bit about what infrastructure protection is doing at a strategic, macro level with regard to information sharing. Right down to the tactical, operational level information sharing environment, the ISE is a process, by which DHS hears information with owner operators, private sector and our state and local partners. There are a number of mechanisms of how we do that, information sharing. But HSIN-CS, again something we've talked about earlier today. Particularly, HSIN Critical Sector, is the architecture that allows us, if you will, to operationalize the information sharing environment between DHS and our private sector partners. We have, I think, we can say, that it's really not your father's HSIN. I'm one of the most vocal critics of the early phases of HSIN and I've heard from all of you, private sector wise, some of the challenges. But I really think that over the past that 12 to 18 months, some dramatic improvements have been made. Nancy Wong's team has been out there and your input and your help has really helped build that portal to where it is now; very robust, over 6,000 private sector partners including the ISACs, including the Trade Associations. That is allowing us to have very broad, deep penetration across all 18 sectors. The HSIN piece really helps us from a macro, strategic perspective of pull, that information sharing piece together with our partnerships.

At a local level, at a tactical level, we talked a little bit about the Protective Security Advisor Program. IP now has 89 PSA's. We expanded 10 states in FY09. We have them in all 50 states and in Puerto Rico, covering the Caribbean. Day to day, programmatically, steady state, their job is to get to know who those critical owner-operators are in their respective regions, to build those relationships with the state and locals, to build those relationships with the owner-operators, to understand that risk and environment in that particular state and region, to build those partnerships, to provide that information sharing mechanism to conduct the briefings, to facilitate the training, to facilitate the assessments, to facilitate the RRAPS. They are our eyes and ears and our ability to reach you quickly and decisively. It's a two-way communication street.

This past year I'd like to think that it's probably been one of the most dynamic years in terms of the threat environment. I don't think we've seen anything this dramatic since I've been at DHS in the early years and since 9/11; a very, very dramatic threat environment. You've read a lot about that in the press recently. Over the past year the protective security advisors, in coordination with Joe Donovan and Turner Madden in the Commercial Facilities Sector, did some very targeted outreach; initialing into shopping malls, to stadiums and now to hotels. The PSA's give us that ability, working at the strategic level with our partnerships and the SSA's and the SCC's and the GCC's to really figure out what that targeted effort should be, who the owner-operators, what information we can put out over HSIN and then what information we can push out at the tactical level with our PSA's, visiting sites developing relationships with those security directors at those particular facilities; and now more importantly, and growingly, connecting those individual security directors with their respective state fusion centers.

This effort is not just have a PSA go out and have a cup of coffee and meet and greet; it is really to go out and engage, offer some services, offer some best practices, the link in local law enforcement, to link in that local fusion center, so that private sector entity now has a local fusion center intelligence capability. That's a big push and a big effort of what's going on during incidents, and there are a lot.

Every day of every year there are literally incidents taking place around the country. Whether they are floods that Julie can speak to, whether they are all wildfires in California, whether there are hurricanes in the Gulf Coast, there are fairly major incidents taking place almost everywhere in the United States at some point and time, and our PSA's become infrastructure liaisons, IL's. They're built into that national response framework. Their job is to coordinate across all the ESF's, they know those areas in those regions. They know those owner-operators; they've worked closely with those state and local law enforcement and state officials.

And their job really is help provide senior advice and guidance to state and federal officials in that joint field office to help looking at the damage state, to help in reconstituting recovery, prioritizing where federal assets and resources should be placed based on the criticality of infrastructure in those areas. So if you don't know your PSA, I would encourage you to please get engaged and know them; we can provide you that information.

I know most of them work with you on a regular basis, but they're a big part of what we are trying to do in terms of bridging that information sharing at the local level.

We are conducting periodic and I'll call them strategic briefings or situational briefings. All of the sectors get regular briefings when they conduct their coordinating council meetings, and part of that is either in FOUO and most cases the classified briefing.

IP has a program where we sponsor security clearances, we've sponsored hundreds and into the thousands of them for their private sector partners, and we want to continue that effort. We are now looking to

take those briefings to the regional level, where there is any threat base or incident base information that needs to get pushed out, to do that leveraging our fusion centers, leveraging our INA analyst, leveraging our PSA's, and be able to do that at the national level with our sector coordinating councils and the PCIS, and they to be able to regionalize that effort.

We've done it successfully this year. I wouldn't say that there haven't been any, a few bumps in that, but it's a new effort. I think it's going to be a very successful effort, a couple of comments on the path forward.

This past April to July IP, Infrastructure Protection co-chaired with the private sector office, an initiative a secretary at the Napolitano Initiative for private sector information sharing, and we visited five cities as part of that effort, facilitated groups, also the PCIS.

As a result of that April to July, five-city tour, if you will, we heard from you. We heard from Fortune 500 companies, trade associations and others that have said, these are the things we think can improve, the information sharing between DHS, the federal government, and the private sector. We've wrapped up those recommendations. They're in a final stage of a report that will go to the Secretary, very shortly, and will go out to you in the near future; I would say by the end of the year.

A couple of items that came out of that report, just to kind of wet your appetite a little bit, a cross-sector information visibility and collaboration; not something we didn't hear this morning, but reinforced in every of the five cities that we visited that we're not stove pipes. Sharing information is important, but cross-sector information visibility and sharing is something we need to do a better job on, private sector participation in all hazards operational planning exercises and evaluations.

Robert, your message has gotten through and it's out there in the hinterlands. We've heard that across the five cities that we went to, and there are, there's a lot of progress I think being made in addressing those things.

Regionalization; one of the things we heard is that the regionalization relationships are critical, that most private sector owner operators do not rely on Washington necessarily to provide them the guidance, the information and the advisories. They rely upon a lot of those local relationships with state and locals and the federal partners at the local level that they've built those relationships with.

And a final comment on educational outreach. Surprising to me, but there is a lot of confusion out there about how DHS, the federal government information should be handled, what are the guidelines for classification, whether it's PCII, whether it's CVI, if it's a chemical or whether it's FOUO. We need to do a better job in explaining to our private sector partners how that kind of information should be handled, and most importantly, how it should be shared and distributed with those that have a need to know.

Thank you.

SUE REINGOLD: Thanks Bill. Guy, over to you.

GUY COPELAND: Thank you very much Sue. I like to know real quickly that when we started the meeting today we introduced people from all of the different sectors, and government coordinating councils and there's a large number here. One of the frustrations for me over the years, in working with all of you and my colleagues and friends and acquaintances here who have been tackling these tough issues, is it's really amazing, literally, the hundreds of companies and government organizations and other organizations that are engaged in this and literally thousands of people, all of whom just can't be here today and get recognized in the same fashion. We should all be grateful for their participation.

I'm particularly delighted because, through this organization, I'm going to talk about a little bit the Cross-Sector Cyber Security Working Group. I had the opportunity to meet and make new friends in many different sectors. The CSCWG, as we call it, just to make the acronym a little bit more pronounceable and shorter, is a unique organization.

In late 2006, early 2007, the National Partnership model was beginning to come together. The National Infrastructure Protection Plan was published. The sectors had either published or were getting set to publish their respective sector specific plans, but there was growing recognition of the great need to do better at cross-sector issues relative to cyber security. So the PCIS worked with DHS and then Assistant Secretary Greg Garcia, to come up with this Cross-Sector Cyber Security Working Group, which I currently have the good fortune to be one of the co-chairs of. Again, it is a joint group. It is government, both federal government and state and local, tribal and territorial SLTT, and it covers the waterfront of all the critical infrastructures, and both the sector coordinating councils where they have them and the government coordinating councils where they have them.

Today, each of the SCC's and GCC's designate who their representatives are going to be to the Cross-Sector Cyber Security Working Group, and the total membership right now is something in excess of 200 plus additional on our mail list for what we call liaison groups that do work or activity or collaboration in the area of the cyber security that's extremely important to either all or many of the sectors. For example, we have close liaison with, and here every month, from representatives of the NCSA's Control System Security Program. For those of you who have an interest in that area, something like Stuxnet might ring a bell. In fact, on this topic, if you had a Windows based PC that was turned on last night, yesterday was Patch Tuesday and Windows, Microsoft released a record setting number of critical patches. You know, my PC was rebooting this morning, I discovered, when I got up because of that, a number of which were to address vulnerabilities that were exploited by Stuxnet.

So cyber security is literally touching all of us, and the Industrial Control Systems Program at DHS has been a superb example of government and private sector collaboration and cooperation in a very focused area of cyber security that's critical to all of us and to many of the sectors. We hear from NCSA's International Program office because cyber

is global. We have to address the issues on a global basis; we can't just to do them within the U.S. We hear from the jointly-run DOD and DHS Software Assurance Forum, which has, participating in it, many of the largest software companies in the U.S. And many of the smaller ones that play very critical roles. We hear from National Council of Information Sharing and Analysis Centers, which Will Pelgrin chairs from whom you've heard earlier today. But that's extremely important for the operational focus. All of the policy and strategy discussion recommendations and work that's done by the Cross-Sector Cyber Security Working Group wouldn't be any good if it wasn't for the operational arms that we're implementing. Policy and strategy should be designed to make those operational arms as efficient and as effective as possible. We hear from the U.S. Computer Emergency Response Team, current issues of importance to many of the sectors. We hear from the Science and Technology Directorate, especially with a focus on their R&D oriented work that they are either funding or following. And we also hear, extremely important to many of us, from the Office of Intelligence and Analysis, to give us good information, or at least the helpful information, regarding what is developing and known about the threat the analysis flowing from that.

Over the last few years the Cross-Sector Cyber Security Working Group has been called on by DHS and by others in the federal government to contribute to the ongoing policy discussions, debate and development. For example, when the President asked Melissa Hathaway to do the 60 day cyber security review for him, the first group that she met with was the Cross-Sector Cyber Security Working Group, even before she had her first joint inter-agency taskforce meeting. And she did, as she later did with other key stakeholders, challenge use with some questions. We setup a tiger team to work on those and provide input to the ongoing study effort.

Many of the recommendations we made appear in the resulting review that was published in May of 2009, and which are being implemented today. Some of those we've already heard about. For example, the development of the National Cyber Incident Response Plan, the focus and emphasis on that. The exercise of that in Cyber Storm III, and now we will continue to be engaged to the Cross-Sector Cyber Security Working Group to make sure that as our subject matter experts develop the After Action Report for Cyber Storm III, we understand what the implications might be for policy, both for government and in the private sector, and make appropriate recommendations to our respective communities; to the end of trying, as I said, to improve it, to make the operational activities as efficient and as effective as possible.

Some other work that this Cross-Sector Cyber Security Working Group has done includes an examination of incentives in metrics. The metrics examination in particular was aimed at helping the sectors as they did their bi-annual updates to their sector specific plans. For the most recent version they had to start rolling in some specific metrics that they were going to track for cyber security. Our metrics report was designed to give them guidelines on how to consider that. One of the most valuable lessons I learned out of both of those exercises, both incentives and metrics, is you cannot take a cookie cutter approach. You can't just write one set of principles or topics or ways to do cyber security metrics and incentives and other aspects of cyber security for each of the sectors, because each of them is quite

different; and as it turns out, for example, something that might be a strong incentive in one sector can be a disincentive in another sector.

So you have to tailor it to the sector's needs and in many of sectors sub-elements of the sector have differing needs and it needs to be tailored specifically to them as well too.

I've been mentioning operational focus and I think that, for some time, has been one of the expressed areas of concern and need within the Cross-Sector Cyber Security Working Group. We have spent a few years pulling together, and putting in place, strategies and policies that we think will provide an environment for operational improvements to flourish, for coordination to improve and information sharing, of a very practical, applicable, useful nature, to take place. And we want to move forward on doing that.

I congratulate Admiral Brown for his focus on that for the last few years; and Deputy Under Secretary Phil Reiter, DHS, and others who've put a lot of focus on pulling together the National Cybersecurity and Communications Integration Center, the NCCIC, the focus on Cyber Storm III for testing the National Cyber Incident Response Plan, and the intent to keep working with us, moving forward, to make sure that our policies and strategies are tweaking and tuned so they will support those very successful operational activities.

Towards that end, we're looking forward to our next CSCWG meeting, which is actually next Monday, and beginning to dialogue with our counterparts at DHS on something that they have as a task now from the DHS Quadrennial Review. Flowing, also, out of the President's 60 day Cyber Review, an update of their policies and strategies for moving forward on addressing cyber security, and the Cross-Sector Cyber Security Working Group and its members are looking forward to working with them on that. Thank you.

SUE REINGOLD: Thank you. We'll turn it over to Will Pelgrin.

WILL PELGRIN: Good morning again. I'm going to talk about three different levels, both from the public-private perspective, a cyber-physical perspective, and a law enforcement and civilian perspective.

What I'd like to do is just go back in time, just a little bit. I can give some perspective of how I got involved in information sharing. First, I think it's part of my fiber to share information, and I define information sharing as sharing of information that benefits, not just me, but others as well. I think, in the past, it was always common that people would share if it benefited their organization. I think that there's been a transformation and we still have a ways to go, but I'm seeing much more sharing when it's not benefiting the entity who's sharing, but the receiving entity that's getting that information.

When I was in New York, in government, I worked proudly for 28 years in government, one of the jobs I held, as I said earlier, was the Head of the Office for Technology. I was in that position during 9/11, and I was the Technical Response. I'm a lawyer by education; I'm not a technical person, but the government wanted somebody who was not fearful of the technology, but was not a technologist, however, during that response and it affected us all deeply and permanently. One of the

things that I saw very quickly was that cyber and physical could never be separated again, and we all recognize that to be a horrific, physical event but what some of us don't know, it was also a major cyber event. In New York State, 250 of our circuits went dark that day. We had a real cyber consequence, and there were multiple different ones that were tangential to that, as well. Based on that, I went to the Governor and I said I really want to concentrate on cyber security issues; can I leave this big agency and start off with a little agency? They said yes; go ahead, which I was very surprised with.

The first thing that we did, I recognized first, through the incredible out pouring of response from the private sector, that we can't do this alone. The government was not. Even though, during crises, everyone looks to government to be leaders, two leaders understanding that you need partners around you in order to accomplish the end state. With that, the Governor called in a series of presidents from major companies to talk about going forward from a cyber perspective, and really learning about vulnerabilities and learning and understanding the critical infrastructure within New York State and really understanding the cross-sector independencies relative to them. To a tee, to everybody that was in that room, they nodding their head, they said, yes Governor, yes Governor and it was just a great meeting. He then turned it over and he goes, well, Will Pelgrin is going to be chairing this. He walked out of the room. Everyone, to the tee, looked at me and said, we're not sharing anything with you.

So I had three options that quickly went in my head, lawyers always have options, right? The first option was call the Governor back in. No, that's not good. The second option, saying you have to. Not good. The third option is the one that I did, which was to say, we worked very well during Y2K; you don't have to share with me. I believe that trust is earned, it's not as a right. I believe that I will share more to you than you give back to me, and that this is a safe haven, which meant that anything shared in this environment would not come back to haunt them later on; and then we went forward. This is now nine years later, and I still meet with every critical sector on a monthly basis. Every year I ask them if they want to continue to do that, every year they say, yes.

From the financial sector, the communications sector, to the agricultural sector, I'm always wearing a national hat as I look at this. My goal is, ultimately, that this should not be New York state specific issue. And with that, we've gone to New Jersey, actually with Cherrie Black, so New Jersey started joining those meetings as well, and the ultimate goal is that it just gets turned over to the National Council of ISACs, where most appropriately belongs. But when they say it can't be done, it can be done.

With that, I had the great fortune of right then, as you recall, right after 9/11 Homeland Security advisors were being assigned to, and developed within, each of the states. They asked me to come in to speak on cyber issues to the Northeast Consortium of them, and I talked about information sharing. They looked at me and I said, would you be willing to share information on cyber issues? You talk about physical issues and they felt very comfortable about talking about physical issues. Would you agree? They all said, yes. I said, I don't mean tomorrow, I don't mean a month from now, I mean literally right away.

And they said, yes; and I said, the other, the only other aspect that I wanted, I said, no non-disclosure agreements initially and no lawyers can be at the table other than me. I wasn't going to play a lawyer at that point, because sometimes that can get in the way. We went for a long period of time without lawyers at the table. I think it was, probably, in our third year when we finally got non-disclosure agreements in place with all the states. I pleased to say we never had a breach of confidentiality.

With that, I started calling every state, trying to find out somebody who I could share information with, because it's not readily available in each state, who that person is. Sometimes I called the Lieutenant Governor, sometimes he answered or she answered, which I was really shocked with. Some of those people stayed as multi-state members. It started small, with 15 states that were at the table. Within, I think, the third, fourth year we had all 50 states. I'm pleased to say we have all 50 states. Local governments are coming in droves at this point, as you can imagine, 39,000 out there. It's difficult to get every one of them at the table. U.S. territories are at the table now, and hopefully soon, tribal governments as well.

The mission of this is how we do this in a collaborative and operative environment. It's not about one way, it's about a common way. It's not about what any one of us can do alone, it's what we can do collectively, and more importantly, it's really a safe haven. You have to have this in a non-threatened environment. Easy, and I'm not sure of which of the panels mentioned about actionable items, but I think it's got to be easy, as well. It's not only actionable; if you're going to share information, it's got to be that I can do something with it. What's the value of that information and make it easy for somebody to get that, and then implement it quickly within their system.

I think it's still too difficult, both from a classification perspective, and I understand why things are classified; but, at the same time, we're the good guys. We need to be able to break that down, get more tear line documents out there. The federal government is doing a tremendous job doing that, as quickly as possible. As Admiral Brown said, getting people classified is a daunting task; but we need to have that if we're really going to have sharing of information that's absolutely critical to have in the hands of people who could make an outcome that's valuable.

More importantly, and I think at the end of the day, is it can't be about a quid pro quo. I can't say, if you don't share information with me, you get away from the table. Sometimes people just don't have information to share and we have to recognize that. We have help people.

One of the things I recognize, in a local government level, is that they don't know necessarily, not all local governments, there's a whole spectrum of governments, you know. Both state and local governments go from being, you know, absolutely brilliant and sophisticated and this to really having very little or no resources at all, and sometimes they don't share or are scared to raise their hand or talk because they don't know what their environment even looks like.

So we have to help them. We have to be part of that solution, and we have to be able to bring them solutions. And so, what we, is a model that we have, is we do it once, but we share it many times. Take my name off, put your name on, become a hero to whomever your respective boss is, as quickly as possible.

Two quick scenarios to show you the really incredible advantages of information sharing, and why it's so critical. I started getting very small stuff. I started an intelligence group. I went to our state police, at one point, and said, you know, we work incredibly with each other; absolutely phenomenal during incidents. We go in together and we can help each other. But it's ad hoc, always, it's never routine. How do we make this routine? So the example I gave is that, you know, we have tons of bridges in New York State. If there is a general threat to a bridge, there's only so much resources that you can allocate to protecting the bridge. What's your analysis or methodology of deciding which ones that you actually deploy resources to? They went through a very complex analysis. And we all know what that looks like, you know, it takes into account human consequence, economic consequence, etc. What's missing from the equation? Well, cyber consequence. What runs under a lot of our bridges? Maybe that bridge, that didn't have, if it was destroyed or incapacitated, wouldn't have a problem from being a diversion of people. It wouldn't have an economic crisis, but it could take down our telecommunications system in a big way. Light bulbs went on, because of that we now meet monthly.

I'm pleased to say, now, the FBI, our Secret Service, DHS at both the I&A and CS&C level, participate as full partners in this. Local police, state police, Department of Justice, and this is an ongoing monthly meeting. Air Force is there as well, I'm just going through the list. The fusion centers are there, Homeland Security Advisors are there; so much so, that the FBI is detailing somebody to our office for an Intel Unit. The state police is detailing, the Air Force is looking into detail; and the whole goal is not to have this replicated all around, but, it's really, we are looking at true information sharing, things that they talk about at these meetings in a very safe way. These things that aren't even under investigation yet, but that may be important if somebody else was seeing it.

The other example was a local college in New York that one of the law enforcement entities got involved with. They asked us to help in a cyber evaluation of the forensics of the service. So we did. If they hadn't shared that with us we would never have found out something that occurred; one of the things that they did, which I think is absolutely historic from the law enforcement's perspective. They had a case, they were getting subpoenas, and generally that's law enforcement sensitive and it stops there. That sharing doesn't continue, generally, very much beyond that, outside of that community. They allowed us to go, our entire membership with the IP addresses of the systems that are out there that were removing data with very strict instructions that they couldn't touch those servers, because there was an active investigation. If we hadn't done that, we wouldn't have found out that 19 states were involved in that.

Absolutely essential that information sharing goes on, and I'm just so pleased that all these walls that we say that were built, they are really not there and they're not hard walls. If we just do it, I think

it's the start that stops most of us, and just incrementally we can make a huge progress. And my time is up, so I'll stop.

SUE REINGOLD: Thanks Will, and thanks to the rest of the panelists. So we'll again, like we did before, move into questions and such. I'd like to give the CIPAC members the opportunity first, and then we'll turn to members of the audience. And while people are getting their ideas, I don't see any questions specifically right now. Why don't I start off just by asking, any of the panelists who want to reflect on this, if you were looking ahead, you know, say to the coming years or such, where or what areas would you like to see additional focus and improvements, in particular, in cyber information sharing? Whether, again, whether that's a focus from a government perspective, from the sector perspective, policy, business processing and technology.

ADMIRAL MICHAEL BROWN: So I'll start. I think it was six months ago, people asked me what my priorities were, and I said, Cyber Storm NCRP and NCCIC. And that remains my priorities, because it's all tied to exactly the question you asked. We now have to go into what I talked about, the repeatable processes, to be able to understand what the individual capabilities and capacities of each of the sectors, each of the department agencies, state and local governments, the individual corporations, so that we can begin to again continue to operate together and understand how as a team we can respond, should we have to. That's going to take a lot of work. It's going to take a lot of development in table talks, in other exercises, so that we can continually look at scenarios that will stress the ability to operate and respond, whether it's steady state, or in fact, in a more significant event.

When you put all that together, it just goes back to what we were talking about. It's about teamwork. It's about getting to the next layer of information, which includes our capabilities and capacity; that that will lead to articulation of what the gaps are, so that we can, once again as a team, try to address those gaps.

GUY COPELAND: I'd like to elaborate on that too. One of the last things that was reemphasized, I think, during Cyber Storm III, was we're beginning to break down the barriers and reluctance for sharing. But now we're beginning to grapple the tougher question of what's important to share. What will I use it for? How can I best use it? What kind of analysis should I be planning to do with it? How can I make that have an impact on networks and systems, etc.

Two aspects that begin to rise to the front; we realize that what we're really sharing is data. We still have to do a lot of work with it in order to have useful information that can be applied and made available in a more general sense, and used by the operators. We're also learning that we need to make the systems for doing that sharing and that analysis a lot easier to use and a lot faster, which means we need to do some innovation, in terms of addressing how to do that and in how to accelerate it and automat a lot of it.

There has been some academic thinking about that, but I think we're going to get, rapidly, to the stage where government and the private sector that, to be addressing that in a very practical sense and beginning to try out and pilot some things for that, as well, so that

instead of waiting for a bi-annual exercise, we can have at least a relatively routine steady relationship where we're sharing information in some assisted fashion so it doesn't put a lot of burden on us.

We have a relatively good common operating picture, and we have those interfaces in place, so that when something does happen we can pick up the tempo very quickly.

SUE REINGOLD: Okay, we'll go to some questions. Also, but just remind folks to, again, just to state your name. Thanks.

ROBERT MAYER: Robert Mayer, Communications Sector. I'm wondering if we could try to use, maybe, a recent example of an event to describe how your organizations have been dealing with real threats. And Guy, you just mentioned, I believe, the Stuxnet, which a lot of us here are aware of and have heard and it affects some really critical sectors.

Using that as an example, can you describe the role that your organizations would play, in terms of remediating something like that, sharing information about it, communicating it to the sectors? To the extent that none of this is classified.

GUY COPELAND: Let me take a quick start at it, but in fact, I'm going to pass the buck a little bit, because I remind you that the Cross-Sector Cyber Security Working Group is a policy and strategy group; so its interest, one was making sure that all the sectors, at least, had the opportunity to understand that Stuxnet was out there, and if it had any impact making sure that they knew where to go to get more information, or to have the kind of private or even classified discussions that they needed to have in order to address it at the operational level.

We did have briefers in to the CSCWG to make sure that the members and the attendees had that information. We also look back at this for lessons learned that we'll fold into the tweaking of the policy and the development of DHS policy in this area as we move forward. And we'll have an ear open to the operational entities, the Council of ISAC, and in particular, some of the more active ISACs like the IT ISAC, the communications ISAC, the financial service ISAC, and the folks who participate in the industrial control systems joint working group, who will give us a lot of feedback and make any recommendations that need to be considered in the policy development.

BILL FLYNN: Let me jump in and give you an example in a little bit of a different area; not cyber, but telecommunications, another important part of CS&C that we work with on the physical security side very closely. Going back a year or so ago, there were some concerns with regard to telecommunications. The infrastructure protection team worked closely with the NCS team at CS&C with the carriers, and collectively identified what were are most important cable landing sites, what are important cable facilities, and our telecommunication hotels in a very collaborative effort with the government and the private sector team helping to identify and prioritize what are those telecommunication assets that we need to be focused on to understand the consequence of the loss to get a better understanding of what the resiliency or the redundancy therein. A lot of good work and some grant dollars were, in fact, pushed to a number of states where these assets

reside to provide them some simple things, such as locking manhole covers, to a much broader range of physical security things that we could address in that area. I thought it was a good example of the collaboration.

WILL PELGRIN: And, just also, that all the ISACs have a daily call with the operational centers of each of their ISACs. So if there's a sector here that's not yet represented on the NCI, please let me know; we'd love to have you at the table. There's no requirement to be an official ISAC to participate, but those daily calls with DHS are situational awareness of what's going on today, and what they're seeing. So it's really, if something like Stuxnet, that's coming up or has happened and one can figure whatever it is, du jour, that, the techies are at the table talking on a daily basis.

SUE REINGOLD: Great, thanks. Go across to Health.

AL COOK: Al Cook, from the Health and Public Healthcare sector. You know with the emergence of the widespread, acceptable of electronic medical records, there are some operational benefits, but there's also an increase risk. My questions to you are:

- Is there any part of your group that's spending any great deal of time on electronic medical records and providing security in that area?
- Is there, or, are you getting sufficient support from our sectors, or some way that we can get additional support for you?

ADMIRAL MICHAEL BROWN: The answer is yes to both. Part of what we're doing is working hard in the inner agency and with NIST in the establishment of standards so that we're taking the approach of the security of the health records in, together with the desire to obviously be more effective and efficient, from an operational perspective.

We've met several times working with Vivek Kundra, from E-Gov, over to ONB, working with HHS together to make sure that as they are going forward, as they are looking at potential regulations, we're working from the security side, from the standard side, to articulate both what the threat is as well as through the use of standards how we can mitigate and reduce that threat. I believe that the sector has been active in that.

GUY COPELAND: Never one to pass up an opportunity, I'd like to extend an invitation to the Health Sector to bring to the Cross-Sector Cybersecurity Working Group, you know, perhaps, a short presentation on the current state of affairs and where that's going, because I suspect that, as we start looking at it, there will be dependencies that the Health Sector on other sectors in addressing those issues. There probably will be implications for other sectors, in terms of what they have to do to respond, to provide the protection and the privacy concerns being addressed, as well.

WILL PELGRIN: I am pleased, up until recently, the Health Sector was missing from the National Council of ISACs. However, they are recently forming into an ISAC and they are represented every month when we meet at our ISAC meetings.

SUE REINGOLD: Okay, over to Commercial.

TURNER MADDEN: Turner Madden, Co-Chair of the Commercial Facilities Sector and past Chair of PCIS. To answer your question of how to promote or how to better improve information sharing, I'd like to see a broader participation and more participation by the private sector. I say that everybody here has drunk the water, and understands what it is too, and the hours you put in, in this system, but I think we need help from DHS to market the sector coordinating council system from the senior leadership. I think an active program to market it would be fantastic. Thank you.

WILL PELGRIN: If I just could give an advertisement. When Admiral Brown was talking about the NCCIC and Guy mentioned it as well, I can tell you, from a sector that was fortunate to have somebody on the floor of NCCIC during Cyber Storm III, and we played in Cyber Storm I and II, it was night and day the benefits of having somebody present right on the floor; just tremendous, and that would not have occurred without the Admiral's vision and insuring that this was integrated operational center. The situational awareness and the sharing that occurred because of our actual presence was just amazing. So, thank you.

SUE REINGOLD: Good, over to Water.

DON BROUSSARD: Don Broussard, Water Sector. I had a question. First of all, I applaud the effort of Mr. Flynn reported about the five city tour to meet with the private sector owner operators about information sharing needs. My question relates to, has such an exercise been conducted within the federal family to find out what other federal agencies or departments information sharing needs are, and if not, is that worth consideration?

BILL FLYNN: The federal agencies tend not to be bashful about, you know, criticizing or coming forward, but I can't say off the top of my head. I'd have to defer to some of my partners in the partnership outreach division to see if there is any programmatic effort to do that. I don't know off the top of my head if we've done that within the federal family. I mean, we certainly meet with the sector coordinating councils on a regular basis, and we capture those requirements; likewise with the PCIS.

There have been a number of initiatives that we've undertaken as a result of that effort. In fact, this past week Mike McDaniel and I met over at the Pentagon, representing the DEB and IP specifically on some of the information sharing initiatives, assessments, data and other aspects of the relationship between DHS and the sector specific agency.

SUE REINGOLD: Good. I'm sorry, on this side I can't see.

HAL DALSON: In the Dam Sector we've developed a tool that we started using. It's a situational awareness-type tool, and recently we've discovered that there are some tweaks that we'd like to see made to it, both through the ISAC section and through the fusion centers. Some of the members of the council are required to report some situations to their regulator. We've worked through the regulator and they have now

allowed us to report security related situations through our SAR tool. Our architect of that is seated back here, so if you have any questions give it to him.

We have had a lot of learning, it was not an easy path. It was difficult for the private sector to actually come to the point where they would use that tool. We've broken that barrier, and I would encourage that, with the Cross-Sector Working Group, what we found is that this particular facility that was reported on was an electrical producer, but there were no links to the electrical ISAC. They don't have a situation reporting tool such as this, yet, but I'm sure was information that they would be interested in that they could go view, if nothing else.

Obviously it was with the Dam Sector, so the Water Sector may have had interest in at least viewing what that report was, so I would encourage that when we go forward we think about how we can make those ties, fusion centers for instance. When we reported this particular incident we had to make four or five phone calls. With information, as Bill said earlier, you have to have it fast, you have to have it accurate. We would really like to see where we could make one contact and it gets out to those people that it has to get to, ISACs would be a primary avenue. We encourage if anybody has any questions, if there is any way we can pull together and at least make one avenue with inputs, outputs, that's something we'd be very interested in assisting with.

Going through the process of designing our information sharing environment, we are a bit of a unique sector, in that, when you look at all of the trucking companies and all the over-the-road bus companies we have out there, we have somewhere around 750,000 possible users of our information sharing environment. That does pose certain challenges in the vetting process. At the same time, we don't rely on a large number of SCADA systems, or things like that, and cyber security is not as large as an issue for us, so much as communicating information about all hazards; but security is still an issue, so I was looking for any advice that you all might have, sort of, on how do we find the balance between betting to make sure that the right people that are the ones getting this information and the ease of use, as for getting online and getting the information to assimilate it.

ADMIRAL MICHAEL BROWN: That's a hard one, really hard, and the going in premise is that cyber security is critically important with respect to the sector, as well as the vast majority of the potential vendors and users that you're concerned about. It's just going to start with the fact that you need to be approaching it from a risk mitigation effort. You need to be able to take advantage of the best practices, start with the best practices, and work your way through there. We're more than willing to help. The reason I say it's hard, is because it's not just the vendors that are part of your sector; obviously, your sector effects everybody, and the implications are enormous, should we not have clear attribution with respect to who the users are and obviously the value of the information that's being passed between all of the users into the sector into the rest of the world. It is extremely difficult even and that's part of where the belief is; starting from the best practices, and working through there, that we'll start to increase the amount of security for you.

BILL FLYNN: I would agree with Mike and I think we can help you on the best practices part. Obviously the sector drives, no pun intended there, but the sector drives who is a member. There are opportunities that tier, you know, what information is available. We can have our team that's worked with, you know, all the sectors in building their HSIN portals, engage, and give you the kind of best practices that Mike was referring to.

SUE REINGOLD: Any other questions from the CIPAC membership before we move over to the audience? Okay, I'll give anyone in the audience an opportunity. Great, if you could please state your name.

BOB CONNORS: Hi, Bob Connors with the Defense Industrial Base Sector Coordinating Council. FEMA is leaning forward a little bit and they've got a three month rotation that's going into the National Response Coordination Center. The intent is not to get somebody fixed there, but to bring in new blood every few months who can, kind of, open up their eyes and see things that are changing. I don't think that's a private sector representative in the National Infrastructure Coordination Center. I believe they're also doing this with the National Counter Terrorism Center, offering a private sector seat.

So my question is, is anybody looking into providing a private sector seat rotational opportunity that may be the person is nominated through the sector coordinating councils, so we can get private sector representation in there, see how things are, now at the appropriate clearances and so forth, but so we can see how things are running and potentially see if there's any other opportunities from an information sharing perspective to improve things?

BILL FLYNN: We welcome your participation in that. We've had private sector participation at the NCCIC; we also have it during incidents in surged events during the, and to imagine so it'll stand up in surge. It varies by sector and how much of that engagement has taken place whether it's, you know, somewhat virtual, whether it's when there's an incident or whether it's steady state. But the fact that we have interest and participation by the private sector in both the NCCIC and the IMC is welcomed.

ADMIRAL MICHAEL BROWN: I'll just jump in. Obviously, as we've been talking about having the connectivity and having the representation, to the NCCIC, is extremely important. Part of what we exercised in Cyber Storm III, was again, increasing our ability to synchronize with the NCCIC and the NOC, with respect to what we had for Cyber Storm III just a on purpose cyber only event.

We recognize that the vast majority of events, just as Will had mentioned, are not going to be either cyber or physical, but will be both, and we need to be able to have that connectivity and response actions. So, anybody that's interested, with respect to what we're doing particularly on the Communications and IT side in the NCCIC, please let me know.

SUE REINGOLD: Any other questions from the floor? Okay, actually I think we're about out of time. So I will thank the panel and turn it back over to the Chair.

TODD KEIL: Great, I want to thank you folks for participating in this panel, and thank the members on the previous panel. I think it was an outstanding and robust discussion, and I particularly was interested in following the questions and some of the responses that were provided.

I also want to thank everybody today for your active participation in the round table discussions; Bill, from the CIPAC side, and the audience. I had specifically asked to deliver my remarks after these discussions to demonstrate; and you notice I was very quiet, which was difficult for me to do. Even Bill kept looking at me to see if I was going to talk, and I wasn't going to. Well, I wanted really to demonstrate my commitment to listening to your ideas and concerns, and to ensure that DHS is being responsive to them and its programs.

I say this often at various meetings. I say in our staff meetings, we look at all of our programs and all of our initiatives and all of our projects in Infrastructure Protection, and we gear them toward what your needs and what your concerns are. There's nothing, I think, more frustrating to me and to our folks in leadership positions than to spend money or time and resources on something that when we finish it, we have a nice glossy book and we probably have something we can show up on slides, and then we talk to you folks, either from the Sector Coordinating Councils or even from the Government Coordinating Council side; and you say, thank you, but really that has no value for us.

So listening to what you have and listening to your concerns is so important for us, and that's why I hope today's plenary session, as well as the dialogue that we promote at our meetings, demonstrates that we are listening and that we seek to incorporate your feedback into our initiatives. Every person in this room is part of a unique partnership. The success of which is dependent upon effective collaboration and information sharing.

As you know, the mission of the Office of Infrastructure Protection is mitigate risk to the nation's critical infrastructure. It's my sincere belief that IP's mission-oriented programs can only be realized when there is full and active participation of both government and industry partners. Given that so many, and you've heard this here today, so many components of the nation's critical infrastructure owned and operated by the private sector, it benefits DHS to determine what it is that our partners need in order to ensure that assets and systems that they manage are both secure and resilient. Therefore, IP will focus primarily on initiatives that you feel are truly beneficial.

For example, one of the most essential parts of securing critical infrastructures, ensuring availability and flow of accurate, timely and relevant information in intelligence about terrorists, threats and all hazards. However, the best way for us to really know what information is relevant to our partners is to work closely with them to understand their industries, their sectors, capabilities and ultimately potential vulnerabilities. When we conduct assessments, host training and exercises, and participate in forums like this, we hope that we end up learning just as much from you as you learn from us.

I really think that today's session is an example of this approach. I learned a great deal today when you look at the discussions we had at both of the panels and the round tables, clearly information and

information sharing is something that is at the forefront. It's something we're spending a lot of time and effort and resources on.

You all want actionable information at the local and regional level, actionable information and we'll put it this way, actionable information that is also easy to act on. True information sharing is something that's crucially important, including information sharing that's multi-directional, and that's something we're working on too.

We firmly believe, and I firmly believe, that one way information sharing is not something that's very effective and very meaningful at the end of the day. With that in mind, I'd like to take a moment to update you on some exciting initiatives in IP that relate to these very topics that we talked about. As we discussed, IP is leading the way in promoting resilience of inter-dependent infrastructure clusters through the initiative which is known and hopefully a little better known and explained today, the Regional Resiliency Assessment Program. The RRAP incorporates DHS and private sector information. It provides resilience metrics, vulnerability and capabilities assessments, and planning efforts to assemble a comprehensive analysis of the resilience of a region's critical infrastructure. The program, as you've heard, is really beginning to take up. It's regionally focused and has real benefits to the public and private sectors. Already we've seen unprecedented multi-jurisdictional and private sector cooperation through the RRAP because everyone recognizes that it has many tangible benefits. My hope is that the RRAP will continue to grow and become a model for how to implement meaningful and critical infrastructure security initiatives across the country. You've heard examples of the RRAP we conducted in 2009, and I believe Don Robinson gave you a list of RRAP that we're doing in 2010 and continue to do in the next fiscal years.

What I discovered when I came to IP and what I heard today, and notwithstanding the mechanisms that we have in place, and everything that we've talked about. The organization does not communicate as effectively with critical infrastructure owners and operators that it could, and it doesn't have a strong enough presence in the field where critical infrastructure is located. It has continued to be my belief that we must work together with the owners and operators of critical infrastructure and our SLTT partners to provide them with what they need, what you need and whether it's information tools, intelligence or training, so that we have collective awareness of the security of the nation's critical infrastructure. Accordingly, and I've talked about this also numerous times, one of my goals is to regionalize IP, to become more field focused and build our critical infrastructure protection capabilities around FEMA's 10 regions. I believe that will better enable the Department to service you, our partners, and the harmonization of IP with FEMA's regions supports the Secretary One DHS concept. And just as important, it will make it easier for you hopefully to work with us.

One area where the benefits of this harmonization will be seen is through exercises with our regional state and local partners. We're committed to expanding the role of the private sector in the development and execution of these exercises, as you heard earlier today. NLE 2011 is an immediate opportunity for this type of engagement. DHS has national and regional planning teams working on

the exercise, and I encourage you and your sector colleagues to get involved as well. This is an area of focus for us as we work to build our regional public private partnerships, so that owners and operators can engage with IP, as well as state and local partners in a collaborative cross-sector environment.

To enhance our ability to share intelligence and other information with private sector partners, we sponsor a Critical Infrastructure private sector clearance program. As you also heard from Admiral Brown, there are obvious challenges with doing that. Right now, Infrastructure Protection has sponsored approximately 1,000 security clearances for our private sector partners. I believe we have about 400 or more. Right now they're in the pipeline and we would like to expand on that program, because it enables the private sector representatives to participate in classified threat briefings and working group meetings where we can have candid conversations about approaches that IP should take on specific matters.

I'll just step back for a second and talk about an initiative that's underway currently, as Deputy Assistant Secretary Flynn said earlier, that's a very dynamic threat environment that we're facing currently. When you see the news from it, started probably a couple weeks ago about the European threat, and possible concerns to the U.S., one of the things we did with our security clearance program is invited our private sector, some of our private sector partners in. We discussed the issue, shared the classified information, and at a discussion at the table, came to a consensus on what we should do with that information. Previously when we had this type of information we and our government, DHS and our government partners, would sit around that table and there wouldn't be a representative from the private sector. We would discuss the issue, discuss the threat information and then we would try and essentially guess the impact that it would have on the sector, or in the private sector and the impact of protective measures would have. Obviously, we looked at that and said, why don't we just invite them to the table? We are sponsoring all these security clearances, let's invite them to the table, share the classified information with them and come to a consensus on what to do with the information.

We started this; we call it the Engagement Working Group. We started this in the spring. We are using it very effectively and, as I said, right now we are out doing briefings in seven cities. The last, sorry New York will be the final city and a classified briefing is going to be conducted in New York this Friday. We just concluded briefings yesterday in Chicago and Las Vegas. So it's a new initiative that we're utilizing and I think the important is not only the utilization of those private sector security clearances that we're sponsoring, it's also that we're involving our partners at the front end. We're not coming out of it when we had a little internal government meeting and informing our partners of what we think is the best approach. We're involving our partners at the front end. This also enables us to collectively develop mitigation measures for identified threats. For everybody now who's interested, you can be nominated for the private sector clearance program. The easiest way is through the Protective Security Advisors, or your Sector Specialist, or Sector Specific Agencies, or any of the IP divisions.

As Deputy Assistant Secretary Flynn talked about earlier, our Protective Security Advisors provide an important conduit of information flow between all levels of government in the private sector. During steady state operations, PSA's conduct briefings and outreach meetings with critical infrastructure partners and disseminate protective measures reports. They serve, essentially, as IP's point of contact in the field and I encourage each of you, as Bill mentioned, to know your PSAs if you don't already know who your PSAs are.

We're also working to build the capabilities of state and local fusion centers, like deploying critical infrastructure analysts to more locations throughout the country. This, we feel in turn, will bolster the partnership between government and industry, because valuable information and analysis will serve as a cornerstone of our partnership.

We're going to implement several other new IP initiatives in the months ahead, and I'd like to briefly just mention two of those, so that you're aware of them. First, we're going to reenergize our national level partnerships by creating an implementation plan for the NIPP that enables us to more effectively track our progress and use metrics to measure our progress. Second, we're becoming more engaged with foreign governments and international organizations, and I think that's crucially important as we look RRAPs and some of the discussion we had today.

It doesn't only stop at the U.S. borders, a lot of what we do, and the inter-dependencies, cascading issues across international boundaries. In the past year we've already collaborated a great deal with the United Kingdom, Canada, Mexico and Brazil, and that experience has increased our understanding of those inter-dependencies of critical infrastructure from a global perspective. IP will also be looking to each of you in the coming year for your advice on these matters, as well as others.

I hope that you leverage your councils to share your ideas and contribute to those initiatives. I think that part is crucially important. It's a very effective means for us to hear what we need to hear from all of you. As you can tell, I'm extremely optimistic about the direction IP is heading.

I'd like thank you all once again for your contributions to this ever important mission of critical infrastructure protection, and for engaging so fully in today's round table sessions. I look forward to continuing to work through the CIPAC to enhance critical infrastructure partnership in the months ahead, and I'm excited for what we have to look forward to in the years ahead.

With that, I will turn the mike over to Clyde, who I believe, has some closing remarks. Clyde.

CLYDE MILLER: Thanks Todd. Well, first of all, let me reiterate that the attendance we have here today has been really gratifying. I wish I could see all of you folks at our quarterly PCIS meetings when we have them. I see some faces that I see quite frequently, and I see some faces that I see every once in a while. I would encourage those of you that are members of your respective sector councils to attend our

meetings. We need the involvement for us to really be effective in all of the initiatives that's been discussed today.

The second thing, is one of the things that, in talking about information sharing and talking about the outreach and everything, it struck me that the correlation is similar to something that was underway years, it's been several years ago now, at a company that actually both Todd and I worked for in the past, Texas Instruments. TI was developing, back then, equipment that could actually finally make the connection between what they call the last mile, to get the broadband connection to people's homes. They could get it to the switching stations in the telecommunications area, but the copper just wasn't robust enough to actually get to the house themselves. So that's when they were developing the digital subscriber lines and so forth, and so on.

That last mile of information sharing, to a certain extent, and that's what I see this initiative being, is that last mile. We've done it at the national level. We're getting better and better at it at national level all the time. Those of us that have specific companies that have a fairly robust communication sharing process internally can do it, as can some of the sectors, but as some of the feedback that we've heard today, all the linkages aren't there yet. I think it's incumbent upon the PCIS, as the cross-sector coordinating council, to work with the councils and the government to make that linkage, get that linkage together.

One of the areas that I think is an area of opportunity, perhaps is, I think, the majority of us in here that are actually owner operators, most likely have contract security alters, contract security staff at our facilities, as kind of the front line of our security presence. I know the commercial facilities sector has taken an initiative here lately of engaging the security companies. We don't have that many security companies in the United States. There's probably, as far as companies that have national presence, there's probably only five to ten of them, but I don't see them engaged directly as those companies in this initiative, so that's another area I see as in our area for opportunity.

I became involved in the sector councils back in late 2004 when I began working for the chemical sector. At that time the focus was all terrorism. DHS focus, totally, was on terrorism, for the most part and the threats that were faced by our nation. Hurricanes Katrina and Rita blew through the Gulf Coast area and made us realize that mother nature was still out there and continued to be a threat that we had to keep in focus as well. By the time we dealt with Gustav and Ike, a year before last, the partnership between sectors and DHS had evolved into more of an all hazard focus.

As part of those all hazard focus, Todd mentioned the classified briefings a while ago. Not only are they providing the classified briefings, but they're also taking feedback. The chemical sector in particular made a request to sessions, we get them about every six months, and two meetings ago we made a request to focus a little bit on Mexico. Are there any terrorists running around Mexico? I don't know, but I can tell you what, I've got operations in Mexico that I'm concerned about. The chemical sector had operations in Mexico that we

were concerned about, as are a lot of the other sectors. They listened to what we had to say in the last two meetings we've had; a big portion of those classified briefings has been dealing with the issues in Mexico. So they do hear what you say. They do respond and respond very quickly in that. As the administration changed, those of us in the private sector, or on the private sector side of the partnership, wondered how the relationship would be affected by the new leadership. I can tell you there were all kind of rumors flying around as to what was going to change and this and that and the other. We saw a lot of new faces arrive and as they began, and watched as they began to put their own stamp on their respective organizations. I can say that we've seen a continuation of an all hazards approach to the mission of DHS and see great progress being made in fostering a clear working relationship with the private sector partners.

Today's program has been an example of the increased collaboration. Today's agenda, and the structure, were developed jointly between DHS and the cross-sector council. Hopefully you found the kind of the different type of structure with the panels informative today. The collaboration has further been evidenced by the efforts of Assistant Secretary Todd Keil. Upon arriving at DHS, to be honest, the first time I met Todd he kind of had a deer in the headlights look about him, but he's recovered very quickly.

TODD KEIL: I still do.

CLYDE MILLER: He's recovered very quickly and he made it clear that his mission to be open and collaborative in information sharing with his partners in the private sector. He's shown time and time again in reaching out for the sector numerous times he's mentioned some of the classified briefings dealing with specific threats that have come up, and discussing not only the details, but how to go about dealing with those threats and getting the information out.

The most recent example of that effort was an e-mail I got on Saturday night a couple weeks ago, saying, can you take a quick phone call? It wasn't like we go out drinking beer a lot, so I figured there was something going on. I was able to hook with him and we had a fairly lengthy conversation about the travel alert that was going to be issued by the Department of State the next day. Todd's also been successful at bringing other federal agencies to the table in some of these information sharing meetings, as we frequently see the FBI and the State Department among others at these briefings.

So I'd like to take this opportunity to thank Assistant Secretary Keil for his leadership and his efforts, as well as for his participation in today's meetings. Quite frequently I see Todd at a lot of the sector meetings and he's there for the duration of those meetings, because he wants to hear what we have to say and he wants to be a true partner; today's meeting is another example of his commitment to information sharing and open dialogue, and I look forward to continuing this collaboration.

Now it's my honor to introduce the final speaker of the day, the Under Secretary for the National Protection and Programs Director, Rand Beers. Rand's also shown his commitment to the partnership with the private sector in numerous ways. First of all, he was directly involved

in the transition between administrations and helped ensure that the office of Infrastructure Protection maintained its focus as the administration changed. He was appointed as Counselor to Secretary Napolitano, I think, back in January of 2009. Then in June of 2009 he was appointed to his current position by President Obama and subsequently confirmed by the Senate.

Mr. Beers oversees the coordinated operational and policy functions of the Director, its five sub-components including physical and cyber, as well as continuing his role as Counselor to the Secretary. He has a long and distinguished career and if I read his bio we'd be here until to 4:00 or 5:00. This guy, it's amazing all the places he's been. He started out as a Marine Officer, served some time in Vietnam, as well as serving in leadership positions in the State Department and on the National Security Council. The numerous meetings I've attended with Rand, he's made his commitment to the private and public partnership abundantly clear.

Please join me in welcoming Under Secretary Rand Beers. (applause)

RAND BEERS: Thank you Clyde. It's always a pleasure to be in the same platform with you. Good to see you again. For those of you who I've known before, good to see you all again. For those of you who are new to this process, welcome. This kind of a meeting at this level of aggregation is, I think, an essential element of the overall approach by the Department and the office of Infrastructure Protection.

We do some things at the micro level. We do some things in an intermediate level and do some things at the macro level, but all of them represent, I think, useful and essential parts of the interaction that must occur between the federal government and our partners in both the public and private sectors around the country; and you all represent the highest level of aggregation of this relationship.

You've had, as I understand, today a number of very useful discussions about a variety of very important issues to you and to us. Clyde, thank you for those very kind words about Todd who has gone out of his way to try to hear you, to listen to you and to take what you say and make appropriate changes and accommodations to make this relationship be a more effective and a better relationship.

And I think, and what I really want to emphasize today, is that the Secretary and some of you have heard this before, came to the Department with a very clear set of ideas about the public private partnership and information sharing. Having sat at the other end of the relationship between the Department of Homeland Security and the federal government as a Governor, through the various things that had come out of the Department and had, in particular, come through fusion centers, she was of the view very much that what we in the Department provide to you, in the public and private sectors, had to be useful, meaningful and timely. In order that 1) you could undertake the broad function that you have with respect to prevention and protection in terms of planning; and 2) that you could be in a position to be prepared to respond to specific or in some cases more general pieces of information about a particular problems and threats.

Now on the one hand if we're talking about manmade, excuse me, if we're talking about natural disasters, to some degree, there is a certain amount of predictability. We know when hurricane "A" is, and we have some advance warning when the hurricane is coming in our direction. We know that there will be floods, and hopefully if you're far enough downstream, you have a little planning time to protect yourself from that; but there are also the natural disasters like earthquakes that we can't predict. There are other things that we have to be prepared for, on the side of manmade disasters, and in particular but not limited to, the terrorist threat, because there are a lot of other crazy people who are not necessarily terrorists who do really stupid and harmful things. We don't have that degree of predictability, and what we are frankly left with is trying to give you the clearest picture that we have of what is possible, and to do it in such a way that does not represent a situation in which everybody is supposed to suddenly throw everything else aside and do everything possible to prevent something that may or might not happen. We've been experiencing that, really, over the course of this past, the latter part of the summer and now into Fall.

I hope, certainly, Todd tells me that the information that we've been trying to give you in a variety of forms and formats including, as Clyde said, the announcement that the travel advisory for Europe for those who are traveling to and those who are American citizens living in Europe, was not something that surprised you, but done in the context of also not wanting to surprise the Europeans at the same time that we were going to issue a document that was going to affect them. So this weekend flurry that we had two weekends ago, but more importantly, as those of you who have participated in the exercises, the table tops, the discussions, the classified discussions, and what not. I hope it is certainly our desire that we are giving you enough useful information that is done in as timely a fashion as possible, so that you can make the decisions that you and your various sectors and firms and facilities may want to make as a result of the information that we are providing you. We are always at risk of looking like we're crying wolf when something doesn't happen, but we also have an obligation to tell you when we think the environment in which we are living in these times is more threatening than it was three months ago, or six months ago.

I've said to a number of you in various settings that if you had asked any of us, who worry about the terrorist threat, to speculate or opine on whether or not the risk of something happening in this country was more or less than at 9/11, I think many of us would have said, really, until last summer that while the threat continued, it was in many ways, diminished. I think the discovery of the plots in New York City, the shootings at Ft. Hood, the airline bomber and the Times Square bomber, we have to accept that the chatter that we are hearing as a general proposition, in fact, has some real tangible potential for occurring in this country, and that we want people to be appropriately focused on things that might make a difference. I think we talk about this in a variety of fashions. The campaign to the general public, but also to the private sector, about if you see something, say something to somebody who can do something about it is part of that effort. I think the outreach that Todd and IP is part of that.

It is a major campaign and one that the Secretary is deeply committed to, given her responsibilities as the Secretary of Homeland Security; I

mean, that is the heart of her mission. And while it isn't all about terrorism, I think that we have to acknowledge today that we are in a different time than we were several years ago, and that we need to take the precautions, so we ask for your input. I hope we're responsive to your input. When we aren't responsive to your input, you can certainly call Todd, and if you're really irritated you can call me.

I notice some of you have already availed yourself of that option and I want to acknowledge those of you who know who you are, that I really do appreciate hearing your concerns. When you can please couple them with constructive suggestions about what we might do to fix the problem that you want to express to me. I really will receive it, even it's only your complaint, and I know Todd feels the same way, because this really is about partnership and we're trying to share the information with you. We expect that you will share the information with us, and we expect that we can do a better job working together than we can working separately.

It is really reminiscent of Benjamin Franklin's aphorism that if we don't hang together we'll all hang separately, and I certainly regard that as almost the motto of CIPAC and our relationship with all of you. If I am the last person keeping you from lunch or departure, I don't want to go on any longer, but thank you all for attending, and I would entertain if there are folks here who have them, a few brief questions before we actually close. So, let me stop talking and if you have something to say, I'm all ears. Thank you.

DON BROUSSARD: Don Broussard, Water Sector. I've been hearing things about the rewrites of some of the National Security directives. Can you enlighten us to anything about that process, like the HSPDs?

RAND BEERS: The normal course of business, from which this administration is not different, is that at the beginning of an administration you go through and you throw out the Presidential Directives that are no longer applicable. You then go through the process of looking at the ones that you have kept in place, because you want the continuity and see whether or not they ought to change.

We are in that process at this particular point in time. Yes, the National Security staff is looking at a number of the Homeland Security directives. There are some drafts of them, but by in large I cannot think of one that has yet risen to the level of decision-making at the senior levels of government at this point in time. Do I expect that to happen? Yes. Can I tell you how long it will be before that happens? Nope. As part of the sausage making process that the U.S. government sometimes looks like. Anyone else?

TODD KEIL: No other questions? Thank you sir, I appreciate it. Thank you for taking the time. (applause)

RAND BEERS: I just want to say thank you again, and I know Clyde's got just a couple closing words.

CLYDE MILLER: I just want to reiterate that I can't believe people didn't take the opportunity to ask Rand some hard pressed questions about whatever. We appreciate you spending time with us and appreciate your words.