# THE CIP REPORT

CRITICAL INFRASTRUCTURE PROTECTION PROGRAM VOLUME 5 NUMBER 4

## OCTOBER 2006

### NATIONAL PREPAREDNESS MONTH CRITICAL CONVERSATION





Contact: CIPP01@gmu.edu

703.993.4840

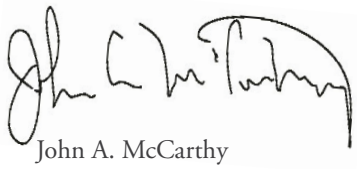
Click here to subscribe. Visit us online for this and other issues at http://cipp.gmu.edu

In late September, the CIP Program hosted a *Critical Conversation* at the National Press Club, focusing on the role of the private sector in the nation's preparedness. This month's *CIP Report* provides in-depth coverage of that event, which featured a keynote by Under Secretary George Foresman followed by a panel of experts moderated by CNN's Homeland Security Special Correspondent Jeanne Meserve.

This *Critical Conversation* was the fourth in a series of events that the CIP Program has hosted over the past three years. The goal of the series is to bring together thought-leaders in the field of critical infrastructure protection and to move the national discussion forward by addressing difficult issues that impede progress. Although there is nothing new about the public-private partnership, we saw a need to examine the relationship and assess its standing. Some of the prominent themes from the September event included the need for a shared vision for preparedness, a concern that the partnership is at a philosophical or inspirational impasse or that it is 'running in place', and a strong sense of urgency in incorporating nontraditional elements of the private sector into the national response planning processes. Speakers at the event endorsed the national planning process and expressed a hope that it will instill a sense of discipline into the public-private sector dialogue to better focus an operational and tactical discussion. (A full transcript of the event is available at www.cipp.gmu.edu.)

In addition to coverage of the *Critical Conversation*, this issue also includes an article on paying for the costs of natural disasters and catastrophic destruction of the nation's critical infrastructure. The authors, whose research was funded by a grant from the National Energy Technology Laboratory, discuss the use of novel cost recovery approaches based on "securitization" and weigh the pros and cons of such approaches.

I would like to recognize the appointment of Gregory Garcia as the new Assistant Secretary for Cyber Security and Telecommunications at DHS. Mr. Garcia joins the department from his former position as Vice President for Information Security Policy and Programs at the Information Technology Association of America. He brings a solid mix of legislative and industry experience and an 'insider's view' of the public-private partnership. We see this as a positive step forward in the nation's critical infrastructure protection agenda, and feel confident that this appointment will result in a stronger focus from all sides on cyber and communication systems security.



John A. McCarthy
Director, CIP Program
George Mason University, School of Law

# Under Secretary Sees 'Teachable Moment' in Nation's Preparedness

On September 27th, the CIP Program, in conjunction with the Department of Homeland Security (DHS), held a *Critical Conversation* as part of National Preparedness Month, a nationwide effort held each September to encourage Americans to take simple steps to prepare for emergencies. This event, held at the National Press Club, explored the role of the private sector in protecting our nation's critical infrastructure.

The Critical Conversation, moderated by Jeanne Meserve, Homeland Security Correspondent for CNN, featured a keynote address by Under Secretary George Foresman and insights from the following panelists: David Eisner, Chief Executive Officer, Corporation for National Service; Paul Kurtz, Director, Cyber Security Industry Alliance; Harrison Oellrich, Managing Director and head of the Cyber, Technology and Intellectual Property Practice, Guy Carpenter & Company, Inc.; David Noznesky, Director of Corporate Security, FPL Group, Inc.; and Johanna Schneider, Executive Director-External Relations, Business Roundtable.

Under Secretary Foresman began his keynote by acknowledging that the public's understanding of critical infrastructure protection and homeland security has grown dramatically in the last five years. Meanwhile, corporate shareholders have increased expectations that the private sector and public sector alike are managing risks to the fullest extent.

Government expectations of the private sector's participation in critical infrastructure protection have been high since the CIP discussion began—there was immediate recognition that the vast majority of the nation's critical infrastructure, and ultimately the responsibility for securing it, is in the hands of the private sector. But 9/11, Hurricane Katrina, and most recently, the foiled plot to bomb U.S.-bound airliners, all underscore the exceedingly high impact that such events have on the U.S. economy, national morale, and the health and welfare of our citizens. The nation at large is dependent on the stability of the private sector, and although the government plays a big role in security, Foresman emphasized that it is not an exclusive role, "because government lacks sufficient resources to be able to protect everybody and everything, all the time, and everywhere." The need for a collaborative partnership between the public and private sectors has never been clearer.

***"On the day before Hurricane Katrina, 25% of the nation's petroleum was produced in Houston, Texas. The day after Hurricane Katrina, 47% of the nation's petroleum was produced in Houston, Texas, due to the number of refineries and capacity that was taken offline in Louisiana."***

Under Secretary George Foresman

The recovery efforts following Hurricane Katrina illustrated some key points in the public-private continuum. A significant focus of the Federal and state response was restoring services such as water, power, and communications. However, these services all depend on a robust supply chain, including airlines, railroad, trucking and shipping—critical services operated by the private sector. These interdependencies complicate even simple recovery efforts. There are no sectors that stand alone; each sector and every aspect of recovery (from clearing a road of debris to restoring telephone service) is interdependent. For example, the road crew cannot be easily tasked with debris removal without operational

*(Continued on Page 3)*

**Foresman** *(Continued from Page 2)*
communications. But repair crews cannot get to the telephone wires if the roads aren't cleared. This is a situation multiplied hundreds of times over in any large scale catastrophe.

***"We can pour in plenty of relief supplies in the aftermath of an event. But until the lights come on and the telephones are operating and the stores are open and people can run down the street and get a little bit of food or a little bit of fuel, you don't start recovery in a community. And when you don't start recovery in a community, you cannot start recovery in a nation."***

Katrina served as a reminder that a natural relationship must exist on the tactical level between the private and public sectors, and on the strategic level between business and government as a whole. Foresman called these interconnections "phenomenally challenging" and stated, "We deal with grant issues every day; we deal with information-sharing issues; and those are complex and they are tough issues. But among the toughest issues that we continue to deal with as a nation is how are we going to protect the nation's critical infrastructure? What is the role of government? What is the role of the private sector? Where is there the ability for collaboration?"

Foresman went on to acknowledge *(Continued on Page 4)*

*Excerpt from transcript*

## Paul Kurtz, Executive Director, Cyber Security Industry Alliance

MS. MESERVE: I'd like to start out by asking each one of you to talk a little bit more about what you bring to this conversation, but also to look ahead from here, where you think we should be in 10 years and what are the real strategic obstacles that have to be overcome. Paul, I'd love to start with you because you said to me on the phone that you didn't think the government would even know if a cyber attack was underway quite possibly.

PAUL KURTZ: I'd be happy to start off. And first of all, I wanted to thank the Under Secretary for his remarks. And I think the piece I might bring to the table is that I agree with everything that the Under Secretary set out today. I think they're all very important statements of the government's approach to the problem, philosophical and inspirational. And I think many of those same statements were made several years ago. In fact, I made them; others have made them in the past. And I think where we ought to be going is into hard priorities and hard programs. And I think one of the things that troubles me is we're not able to go through and identify hard priorities and hard programs that affect the protection of all the key infrastructures across the United States.

And that's not to say that the Department of Homeland Security is not doing anything. In fact, I think George and others could talk about the CIP grant that has been given to cities and municipalities to help them shore up their information infrastructure. But we should be moving to a place where we're talking about the programs that have been set up and, if you will, debating whether or not those are in fact the right programs – kind of, if you will, if you look at where we are with DOD, we debate about what kind of aircraft we should have for the future. Does that impact the light aircraft in our defense? We are not having those very specific debates about programs and critical infrastructure protection. And we need to get there sooner rather than later. I would argue we've largely been running in place. We've had some progress, but we need to get more specific about what we want to do in the future.

MS. MESERVE: One of the comments here has been communication, both from the Under Secretary and all of you. But, do you even know who to talk to? Is it clear who in government plays what role, what their responsibilities are, who the go-to people are? Why don't we start with you again, Paul?

MR. KURTZ: I think the answer is yes and no. I think at an everyday level – let's get specific – in the IT community, there are a set of points of contact that the private sector can go to at the Homeland Security department to talk about IT issues.

I think where it gets more interesting and of greater concern is what happens if we have a more significant event where we've graduated from the noise of every day. We have something going on in the networks that it requires more senior level attention around government, not just at the department of Homeland Security, but DOD, the FCC, on up the line. You get into how do we *(Continued on Page 8)*

*Excerpt from transcript*

## David Noznesky, Director of Corporate Security, FPL Group, Inc.

MS. MESERVE: I'd like to start out by asking each one of you to talk a little bit more about what you bring to this conversation, but also to look ahead from here, where you think we should be in 10 years and what are the real strategic obstacles that have to be overcome. David?

DAVID NOZNESKY: Well, I heard Under Secretary Foresman and actually took some very profound things relating to public-private partnerships. Having come from both sectors, the private and the public, they really do have a hard time talking to each other, and in fact, not only did they not speak the same language, but for some reason, culturally in the government, it's very difficult to speak in that language to the private sector.

But I think some positive things have happened in that partnership. First, for a challenge, our industry, in particular, Florida Power & Light Company, is well versed in disasters and the challenges that they present. So culturally, we know that those relationships with the state and local governments and the federal government are critical before a disaster. And if there's one thing that I could say to companies is that in business, continuity planning, it is absolutely critical to develop those relationships and those dialogues before.

I think for corporate security officers today, one of the biggest challenges is business continuity, crisis management, and certainly 9/11 brought a whole new focus and dimension to what is business continuity. And I think in the area of improvements, I think we've seen recently the development of the National Infrastructure Protection Plan and also the private sector specific plan has done a lot to improve the partnerships between our industry, and the input our industry has had with the Department of Homeland Security.

So I think strategically, those dialogues have to continue; those relationships have to continue, and that will be a critical part of being able to continue and be resilient. Undersecretary Foresman said you can't protect everything everywhere every day, and of course, in our industry, that's critical, because you have to be resilient. You have to have good restoration planning.

MS. MESERVE: David, you seem more or less pleased with the state of play, but do you have any suggestions for further improvements on how to do better?

MR. NOZNESKY: Well, I think a number of things over the last few years have been progressing and are slowly being implemented. I would like to emphasize some of the improvements, some of the positive things that have occurred.

And I think one area in particular that relates to the power industry is the National Infrastructure Protection Plan. I mentioned that earlier. But the reason why I wanted to bring that up is because there is a sector-specific plan that is included in that. And that was I think one of the best examples in the last two or three years to show that public-private partnership, *(Continued on Page 15)*

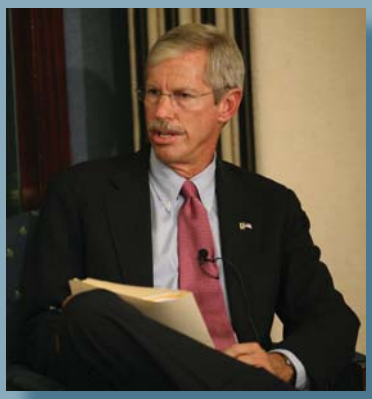
**Foresman** *(Continued from Page 3)* that although the security challenges faced by the private sector often equate to national security challenges, the Federal government cannot instruct the entirety of the private sector on how they should best manage their risks—the private sector owns these challenges and may choose a different path to a secure end state than the government might take, but Foresman added, "…that's okay, as long as we arrive at the same destination."

After recognizing some of the biggest impediments to critical infrastructure protection, the Under Secretary stated that it is time to change the national dialogue from one of challenges to one of empowerment—what is empowering us to make more and more progress on a daily basis.

Every business has legal, economic, and humanitarian reasons for appreciating the importance of preparedness. Factors such as customer service, reliability, earnings, and shareholder confidence drive business continuity strategies that feed into preparedness. However, no single company, industry, or even the private sector as a whole can address the realities of catastrophic risk without new levels of public-private collaboration. Foresman stated that he wants to institutionalize a preparedness system for catastrophic incidents that transcends current capabilities that have been mastered in dealing with more localized emergencies and disasters. Although national catastrophes have a lower probability of occurring, they have higher consequences, and must be addressed seriously *(Continued on Page 5)*

*Excerpt from transcript*

## Harrison Oellrich, Managing Director and head of the Cyber, Technology and Intellectual Property Practice, Guy Carpenter & Company, Inc.



MS. MESERVE: I'd like to start out by asking each one of you to talk a little bit more about what you bring to this conversation, but also to look ahead from here, where you think we should be in 10 years and what are the real strategic obstacles that have to be overcome. Harry, I think all of us probably turn to you if there's a crisis.

HARRY OELLRICH: Well, I do view us in some respects as analogous to first responders in a tangible sense in that when bad things happen, basically you look to either government or to the insurance and reinsurance industry to maintain or to preserve liquidity. And I think that's something that gets lost in the translation in much of the debate that goes on relative to whether our sector's companies are doing what they should be doing, doing all that they should be doing, etc.

Maybe I should back up a bit before I move forward though and just indicate – because I think what I do for a living is slightly less intuitive than some of my colleagues here on the panel. I represent a firm by the name of Guy Carpenter & Company. We are reinsurance, not insurance brokers or intermediaries. Our clients are the major insurance companies worldwide. All insurance companies, from the smallest single county mutual, right on up to the major multinationals basically purchase reinsurance to be able to manage their risks.

They specifically buy it in the context of today's discussion to protect against untoward or unacceptable accumulations or perceived accumulations of catastrophic exposure, be that to earthquake, to hurricane, to cyber, to a whole host of other events, both known and unknown. And really, to be able to get insurers to play that role and to play it to a greater extent – reinsurers to sit above them and support them – we really need to be in a position in ten years to be able to be working very much more closely with everyone who is a stakeholder in this debate, everyone who has a horse in this race, in that we don't have all the answers.

Our industry has basically spent the last decade or more reaching out, trying to develop some pretty sophisticated models to be able to try to sort out what our maximum foreseeable or probable maximum loss might be in *(Continued on Page 10)*

**Foresman** *(Continued from Page 4)* so that the nation is truly prepared in the event of a catastrophe.

In order to implement this preparedness system, Foresman said that we need to answer three questions:

1.) How can government at all levels better communicate and coordinate with industry to manage catastrophic events?

Foresman stated that consistent and accurate information is absolutely critical for more productive preparedness and response, including both boots-on-the-ground operational issues as well as long-term strategies for physical and economic preparedness. Communication channels must be in place prior to any disaster so that the nation is prepared at a sophisticated level. The government must do a better job of educating senior decision makers in the private sector about how the government prepares and responds to catastrophic events so that they can in turn establish accurate expectations for their employees, suppliers, vendors, and shareholders.

The strategic relationships between the Federal government and industry are very important. However the relationships between state and local government and local and regional businesses are just as critical because decisions made at the Federal level will be carried out at the local level. *(Continued on Page 6)*

Jeanne Meserve, CNN Homeland Security Correspondent

**Foresman** *(Continued from Page 5)*

"Ignoring government authorities and plans is not an acceptable solution," Foresman said.

John McCarthy, Director
CIP Program

"Government cannot bury its head in the sand; corporate America cannot bury its head in the sand. We must work collaboratively. But by the same token, government is unable to manage catastrophic events without harnessing the full value of our relations with our private sector partners."

"Clearly communicating our respective rules of the road, our strategies for preparedness and response, and our needs are all conditions for success and overcoming the communications challenges that we face."

Foresman identified the National Response Plan as an area requiring special attention from industry. The Plan is being updated and is based on the idea that incidents are typically managed at the lowest geographic and jurisdictional level possible, and that incident management activities use the principles contained in the National Incident Management System. Foresman stressed that the National Response Plan must be more robust and must integrate public and private sector responses to catastrophic events. *(Continued on Page 7)*

*Excerpt from transcript*

## Johanna Schneider, Executive Director-External Relations, Business Roundtable

MS. MESERVE: I'd like to start out by asking each one of you to talk a little bit more about what you bring to this conversation, but also to look ahead from here, where you think we should be in 10 years and what are the real strategic obstacles that have to be overcome. Johanna?

JOHANNA SCHNEIDER: To answer your question, where would we like to see things in ten years, we've looked at this from all angles. Our companies were very generous in the immediate aftermath of Katrina in trying to help the nation recover – first, save lives obviously, but secondly, try to recover as quickly as humanly possible. The lessons that we learned were that to really impact things in the future, we needed to organize ourselves most effectively, first and foremost. We needed to be able to provide to the government an integrated business community so that when the government needed us or when there was a catastrophic event in the United States, we were able to bring to bear all of our full resources.

So what we're working on – and we may get into this further – is trying to leverage our own company strengths, our own cross-industry disciplines, so that when there is a catastrophic disaster – again, to George's point – there's never a routine disaster, but there are certainly issues that are so catastrophic, you would expect the corporate community to bind together and to be able to respond as one.

One of the problems that we identified in 9/11 and in Katrina was you had the tendency, as government, to try to identify and pick off, so to speak, businesses that A, you're familiar with, or, B, have come to the fore in the past. We need to be able to provide to NGOs, to the government, a united front, so to speak. So business has already done the hard work of educating our employees, our CEOs, and all of our senior executives – and then, preparing, drilling, and being ready when a catastrophic disaster comes to bring to the table a very specific set of resources that we can provide to assist in a national recovery plan.

MS. MESERVE: Johanna, you mentioned to me that you not only, of course, have to interface with the federal government but you also have to play with the state and local governments as well. How do you effectively do that when you've got a private sector that represents thousands of industries with things to offer? How do you communicate? *(Continued on Page 11)*

**Foresman** *(Continued from Page 6)*
The goal of the Plan is to provide the structure and mechanisms for national level policy and operational direction for an all-hazards approach to incident management.

2.) How can the public and private sectors clearly define and participate in a shared vision of catastrophic preparedness?

Foresman stated that he believes most communications challenges stem from a lack of a shared vision for preparedness and response to catastrophic events, and sees this at the core of the divide between the public and private sectors. Even more refined communication and coordination would not deliver a shared vision and clear expectations. He said that 9/11 presented a teachable moment to lay the groundwork for a national approach that integrates prevention and protection with response and recovery. Foresman continued, "Hurricane Katrina showed us that despite 9/11, we continued to lack an integrated national approach for managing the full range of risks that we face."

But Foresman emphasized that the nation has made progress, citing the after-action reports published by the White House, Senate, and the House on Hurricane Katrina, the implementation of many of the recommendations by the Department, and the commitment by the Administration to hold people accountable for progress. The private sector and state and local governments continue to do an exceptional job every day in dealing with the vast majority of emergencies. But *(Continued on Page 8)*

*Excerpt from transcript*

## David Eisner, Chief Executive Officer Corporation for National Service

MS. MESERVE: David, you have been down there in the Gulf Coast looking at it up close. What impact has insurance had, could insurance have in that recovery?

DAVID EISNER: Well, when I look at it from an insurance point of view, I look at it a little bit differently from the reinsurance perspective. What I have been seeing in both Mississippi and particularly in New Orleans is an incredible amount of confusion because the insurers all have different policies around what constitutes hurricane damage and what constitutes flood damage. Generally the wind damage is considered covered; the flood damage is not.

It becomes a pretty academic exercise, and right now, I think one of the big challenges that a lot of residents are having, and a lot of whole communities are having, is trying to figure out whether their losses will be covered or not.

MS. MESERVE: Tell us how we address it. What is the plan?

MR. EISNER: Well, I think the most important thing is to be able to operate at several different levels. It is really important for us to build the relationships, improve the National Response Plan so that we all understand what we are going to try to do together to make sure that the business community is coming together, that the non-profit community, that the government all have these plans.

But at the same time, it's really important to recognize that you can't use this plan as a bottleneck. It can't be that if someone says I can fix that problem that they have to go through this elaborate process that has been prescribed. When I was at AOL during September 11th, one of the things that we did that was most effective – the Blackberries were working; the phones and the radios weren't. We just made thousands of Blackberries available to the police officers and fireman, and then later we worried about making sure that all of the managers and the folks understood it.

So it's really important to be able to operate both at that sort of planning-coordination level to maximize the chance that your plans are going to have an impact, but not create a culture where businesses or private citizens or government somehow believe that the plan itself is going to fix everything. One of the things that we learned is as strong and as good and as well prepared as we are, there is going to be things that we are not ready for, and something like catastrophe will require all of us to use all of our best assets.

And we have to be really careful – I think one of the big mistakes we made was we felt that because we were all signatories of the National Response Plan, and because we knew this National Response Plan could hit certain benchmarks, we kind of over-relied on it. *(Continued on Page 16)*

**Foresman** *(Continued from Page 7)*
without a shared vision for catastrophic preparedness and response, it is difficult to get to where the nation needs to be.

Foresman urged the public and private sectors to come together in a new covenant for a shared vision that will last for generations to come, a covenant "steeped in deep notions of trust, respect, and clarity of vision." A shared vision would embody several principles held by both government and industry: first, a deep concern for the loss of life; second, a deep respect for public trust and confidence in our institutions, economy, and way of life; third, recognition that the public and private sectors share common risks, including threats and vulnerabilities, and thus share a common responsibility.

"Finally," Foresman continued, "this covenant would acknowledge that the management of catastrophic events will not be easy, but the risks of going it alone or not doing anything are simply not acceptable. The American public expects more; the American public deserves more."

3.) If we are able to communicate and come together with a shared vision, what are the specific short and long term solutions that merit prioritization?

The primary challenge Foresman raised was integrating public and private sector plans for catastrophic events. He acknowledged that many organizations have sophisticated plans in place already, but that industry and government must socialize their plans into a collective framework. In order to do this, both sides must be comfortable with a number of concepts and protocols.

First, the private sector must compete on market principles, but collaborate on security needs. Second, government at all levels must bridge jurisdictional boundaries in order to harness the power of collective skills and services. Third, public and private sectors must set clear expectations and negotiate together, so that plans and protocols are integrated into a single national approach.

Foresman concluded his remarks, saying "we have an opportunity in the post-Katrina environment, in the post-dustup environment of a whole lot of things, to recommit ourselves to this public-private sector collaboration and to recommit ourselves to truly working through these challenging issues, because I've got to tell you, something is going to happen. It may be tomorrow. It may be next week. It may be next month. And if you're from government, your citizens will expect performance. And if you're from the private sector, your customers and your shareholders will expect performance. Our job is to make sure that we deliver on those expectations." ❖

**Kurtz** *(Continued from Page 3)*
do command and control during a crisis when it involves the IT infrastructure, and the communications infrastructure? I think there is not enough clarity as you escalate up the line as to who the real decision-makers are as we go forward. And I know the BRT's report has talked about getting into recovery and reconstitution issues – that's where we have some real gray area that we need to clarify roles and responsibilities as we get into a crisis.

MS. MESERVE: Paul, there are networks set up. There is the ISAC system where there is supposed to be trading of information between the government and the private sector. There is the Homeland Security Information Network, and so forth. Do these channels work? Are they able to overcome these obstacles that have been mentioned, these obstacles of language and cultures that exist?

MR. KURTZ: I think to a degree they work. And I think the IT sector is pretty interesting space. The IT sector has set up something called an Information Sharing and Analysis Center where members of the private sector have come together to exchange information. The IT sector has set this up at its own expense, if you will; it's not supported by the federal government, and it's been around for several years. And they have been able to develop protocols for sharing information. They have engaged in non-disclosure agreements so that they can share information securely.

What is problematic – there are two issues that I think manifest itself. First of all, the government has, if you will, kept the ISAC, this ISAC and I think others, not all, at arm's distance. And so – and to *(Continued on Page 9)*

**Kurtz** *(Continued from Page 8)*
give you an interesting example, in the context of the London bombings last year, there were a lot of the ISACs that were wondering what in fact was going on. Did we have a problem here in the United States? What were we doing?

And a bridge was set up among many of the ISACs very early in the morning around 7:00 a.m. when news of the London attack came out. It wasn't until several hours later that the Department of Homeland Security was able to come out with its statement on what in fact was going on, but the private sector had in fact shared information in advance. They had started to develop the trusted communications channels and the lexicon in order to deal with each other during a time of crisis.

What I think is interesting also about the IT sector with regard to lexicon, when we have an event, and we will have an event, a large-scale event involving the IT sector, remember that geeks will be fixing the problem. The other 99.99 percent of us will be standing on the sidelines because the software engineers, the enterprise architects – all of those people will have to be delving into the details, which means everybody else won't have a clue as to what is going on as people try to sort these out. And when the Department did its Cyber Storm back in February, one of the issues that came out of the after-action report was an issue of lexicon.

So you have senior people sitting around and all of the geeks are doing their geek talk, and they have to translate this up into what it means to the policy makers, what in fact is happening on the networks, what it means as far as response, and recovery. That is where I think exercises are incredibly valuable, and the Department should be commended for putting together the exercise. We need more of those on a more localized scale as well; they don't all have to be national in nature.

***"We are not having those very specific debates about programs and critical infrastructure protection. And we need to get there sooner rather than later. I would argue we've largely been running in place. We've had some progress, but we need to get more specific about what we want to do in the future."***

MS. MESERVE: Paul, there has been a lot of criticism on the cyber front for the government, that they just haven't been paying attention, they haven't grappled with it. Why do you think that is? Is it because they don't understand it? Is it because it's so large they don't know where to begin, or is there some other answer?

MR. KURTZ: I think those two reasons are valid. I also think it's fair to say that the Department has had some significant challenges since it started up. One, 22 or 23 agencies coming together is not an insignificant problem - all of those agencies with different cultures. Secondly, you can add Hurricane Katrina on top of that, which was obviously a very significant event for the Department, the Federal government, and state and local authorities.

Beyond that, we continue to have intelligence about attacks to the physical infrastructure, attacks that would kill people. When it comes to the information infrastructure, it's kind of hard to get your head around it. One, you can't really see it, you can't really smell it, you can't really feel it, but it runs everything, and so it's almost a feeling, if you will, of "it's too big to fail." It will always be there in some form or capacity, and those who say it may go black or something like that, or hype up the problem, you know, that in fact could happen. I think a more likely problem is that we'll have a loss in bandwidth issue.

But I think there has been a series of things that the Department has had to deal with, and this has consistently been on the bottom of the list. Now it's starting to move up. But let me put a marker down. I think today, this week, we have another potential problem in front of us. As the Congress is debating the reorganization of Federal Emergency Management Agency (FEMA), there is discussion about having the cyber and communications division over on one section and FEMA over here, but having recovery and reconstitution rest within FEMA, which is essentially splitting out recovery and reconstitution from situational awareness and prevention efforts. It doesn't make a lot of sense.

When you look at an organization like the National Communications System, which has been around since the mid-'80s, they have had situational awareness and recovery / reconstitution together for a long time. And you could argue that is good. Now we may have the Congress rip it apart. That is not a good idea. It puts people like Under Secretary Foresman in a very bad position and puts the private sector in a nasty position of who do we call at the Department? Do we call someone when it comes to prevention and protection, and we call someone over here for response and recovery? It's not clear. We hope it shakes out properly. ❖

Oellrich *(Continued from Page 5)*
any real or hypothetical event. And we don't have all the answers. The government has data that we probably can't even imagine if we could mine it or know where to turn to be able to work with them to mine it.

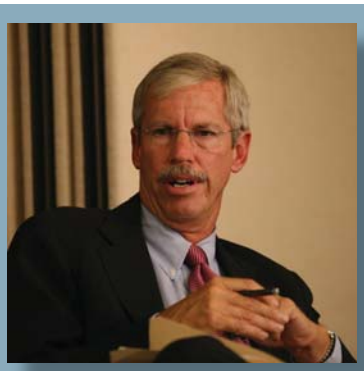
***"Our industry has basically spent the last decade or more reaching out, trying to develop some pretty sophisticated models to be able to try to sort out what our maximum foreseeable or probable maximum loss might be in any real or hypothetical event. And we don't have all the answers."***

If we can do that, if we can build even more sophisticated models that will help to provide insurers and reinsurers with additional confidence that they can figure out what their loss could be by entertaining certain exposures, they'll write more. Or maybe they'll write a lot of those exposures and over time, we build out a much more sustainable and long-term and robust market that can also basically help to harden infrastructure in and of itself because what it does, it will basically create best practices, if you will, that an individual firm or an individual would need to be able to have to be able to either afford coverage or to be able to procure coverage in the first place. So we think that we can play a fairly prominent role if we're able to work even more closely with government than we have in the past.

MS. MESERVE: Harry, I wanted to delve into this insurance issue a little bit more. You have explained how the insurance industry is a little reluctant to write this kind of coverage because they can't quantify the risks. Harry, you mentioned that the government may have data that could be helpful. What do they have? How do you think you can get it?

MR. OELLRICH: Well, this is really the $64,000 question. There are so many different places within the bowels of government, so to speak, that data that could conceivably be directly useful, it could be used as a proxy for something that we might be able to build in conjunction with government, a model particularly in the cyber area. I mean, we have a tremendous second chance here, and that, to Paul's point, it hasn't happened. It's likely that at some point in time it could happen, and, you know, it's very difficult to get insurers any exposure to cyber or bricks and mortar tangible exposures if they can't predict with some semblance of rationality what kind of a loss might result from a particular event. They are not going to be able to convince their board that it makes sense to be able to write very much of that exposure at all.

And because of that, if we can find a way to access things that government might have, individuals – the ISAC is great – they are more tactical. I'm thinking in a strategic sense, the ISACs deal with threats. I'm thinking about dealing with things that can physically be used to embolden insurers, to do more of these kinds of coverages, and by doing that, create those best practices. Like the factory owner that basically uses insurance. He needs to have insurance; he is told that he has to have insurance to be able to remain in business. He doesn't necessarily sprinkler his factory because he is a nice guy or out of some altruistic virtue; he does it because he knows that he can't afford coverage or he can't get coverage at all without it, and without it, he is not allowed to do business. Well, very much the same thing can happen with other product lines that can, by definition, pull the entire infrastructure of the country up by its bootstraps by adopting those best practices.



MS. MESERVE: In the meantime, Harry, what is a business to do?

MR. OELLRICH: Well, that is an interesting question. I think one of the first things that you need to do, because it's very likely that when push comes to shove, you may not be able to have or you may not be able to secure all of the coverages that you would ultimately need. Therefore I think it behooves every business to really get out there straightaway and assess what their exposures are, and to basically mitigate those however they can.

I mean, this will sound like an advertisement to some degree, but you need to be able to have an advocate on your team. Large companies are able to have either risk departments or a risk manager on staff, and even those major companies use the services of major specialists, brokers, for instance, that will basically come in, will assess your exposures, they work in that space every day; they basically can take a look at what you have, look at your coverages, hand tailor coverages, tell you what you need, and then be able to secure them at an efficient cost. That provides belts and suspenders to some degree in terms of knowing that you have what is available at an effective cost.

The smaller companies and the mid-size companies may not have the luxury of having those specialists on staff, so it becomes even more important for them to be able to bring a professional in who does *(Continued on Page 15)*

**Schneider** *(Continued from Page 6)*

MS. SCHNEIDER: Sure, well, the long and short answer is it's a work in progress. Really, there is no one place to call, to pick up the phone. There is no 1-800 number to call for a variety of companies, for industry, for commerce. What the Roundtable has tried to do, and our companies have asked us to play this role, and we will see if we're effective and successful, is to essentially be a broker – to allow our companies to call us and for us to triage calls to the federal, state, and local.

We're undertaking an effort to work with the Emergency Operations Centers, which, as you know, are the key component in each state. Every disaster, every catastrophic event happens somewhere, as George said in his speech, and that somewhere usually has boundaries, has state officials, has a governor. So we are trying to do both – the bookends. We're trying to make certain that the federal government understands that we're a resource and we can be accessed for companies to get information from the federal government, but also to go to the state and local. I don't know that you'd ever find one1-800 number to call, but certainly you can identify at least three or four areas of the most pertinent information.

MS. MESERVE: Johanna, absent this insurance at this point in time, this kind of coverage, what should a CEO do? How do they protect themselves? Is there some backstop that should be created?

MS. SCHNEIDER: Sure. Well, CEOs clearly have a fiduciary responsibility to protect their employees, to protect their physical assets in any type of a disaster or an event. So they owe it to the shareholders, they owe it to the employees, and that of course is their first and primary responsibility. And to that point, you should all know, every company has continuity plans. They practice those continuity plans, they prepare, they are very well educated. So they know if something were to happen to this company, the employees all over the country – here is how we recover, here is how we connect. So they have, as I said, a fiduciary responsibility.

Beyond that, in the greater sense, what we are really talking about is I think a tremendous economic potential for disaster for this country because if you do not have reinsurance, and if you do not have insurance, and you have a major event, at some point, there will be public pressure for the government to step in to provide that backstop that is necessary. That of course would create a tremendous impact on the economy. There would be deficits; there would be an issue of fairness. And so I think it's only prudent that we all have to come together and try to look at what is the reinsurance market, what is the insurance industry's role?

MS. MESERVE: Would you think that government should have a rainy-day fund at the ready for this sort of catastrophe where they might have to step in?

MS. SCHNEIDER: I think from an economic standpoint, they need it.

MS. MESERVE: Johanna, what is your wish list?

MS. SCHNEIDER: Well, back to information is king, we amassed a tremendous amount of information on the corporate side following the tsunami, Hurricane Katrina, Rita, Wilma, Stan. Next week we will be announcing a website, a public website, www.respondtodisaster.org. We have taken all of this information and put it into the website. It explains to the average – no acronyms – to the average reader what is the role of the Federal government in the midst of a disaster, what is the role of a state and local government, what is the role of a corporation, what is the role of an NGO. We list in an encyclopedic form, every NGO, what they do, who to contact, what specific role they have to play. So we think this will help small businesses, large businesses. This is for the public to become educated about disasters.

> ***"We needed to be able to provide to the government an integrated business community so that when the government needed us or when there was a catastrophic event in the United States, we were able to bring to bear all of our full resources."***

Again, back to your point, precisely, if you can become educated prior to the day of the disaster, you will perform much more efficiently during the disaster. So first and foremost, we are trying to provide a public service through the website, and then secondly we are trying to coordinate all corporations across the board so they have an input through the Roundtable so in the event of a catastrophic disaster, they can leverage each other's expertise, go through the Roundtable, and get to the government.

MS. MESERVE: Will competitors cooperate in this field?

MS. SCHNEIDER: That is a great question, and of course antitrust is always on the minds of every corporate lawyer, and we have, and are continuing to work through – but, yes, I think the bottom line is the CEOs have told us they think they have worked through it, and, yes, they can both coordinate and collaborate. ❖

# Paying for the Costs of Natural Disasters and Catastrophic Destruction of Critical Infrastructure

Michael E. Ebert, Principal Research Associate, CIP Program
James B. Atkins, Ph.D., President, Regulatory Heuristics, LLC and Senior Consultant to the CIP Program

During 2004 and 2005, a series of destructive hurricanes struck much of the Gulf Coast region of the United States resulting in catastrophic damage to the regions' electric infrastructure. The destruction from these storms resulted in billions in damages and subsequent repair costs to rebuild and restore the reliability of the electric system to pre-storm conditions. Historically, self-insurance mechanisms such as storm reserve accounts and monthly surcharges added to electric customers' bills have been adequate to recover the uninsured losses of investor-owned utilities (IOUs) resulting from storm repair costs. However, the 2004 and 2005 hurricane season inflicted such catastrophic energy infrastructure destruction in the Gulf Coast states that storm recovery costs far exceeded the available funds in individual IOU storm reserve accounts, resulting in very large deficits. To exacerbate the financial recovery process, many parts of the Gulf Coast, such as New Orleans, remain without fully reconstructed electric infrastructure a year after Katrina, resulting in significant shifts in electricity usage and associated customer revenues. Financing such storm repair debt and paying for the excessive recovery costs has presented immense financial burdens and regulatory challenges to IOUs, state public utility commissions and customers.

As a result, state legislatures, Public Service (Utility) Commissions (PSCs) and IOUs have begun to implement novel cost-recovery approaches based on "securitization" to repay the IOUs' recovery and repair debt and to fund storm reserve accounts. The use of storm cost recovery bonds in the Gulf Coast region represents a dramatic change in state regulatory policy. Due to the far-reaching policy, regulatory, and critical infrastructure implications, the Critical Infrastructure Protection Program (CIP Program) at George Mason University School of Law in May 2006 launched a research project examining and comparing recent changes to natural disaster cost recovery approaches in Florida, Louisiana, Mississippi, and Texas under a grant from the National Energy Technology Laboratory. A preliminary report, "Critical Electric Power Infrastructure Recovery and Reconstruction: New Policy Initiatives in Four Gulf Coast States After 2005's Catastrophic Hurricanes," was recently provided to the Department of Energy's Office of Electricity Delivery & Energy Reliability.

Securitization refers to the creation and use of a new type of bond issue that falls within the general category of asset-backed securities and its subset, utility tariff bonds. The underlying securitization statutes in Florida, Louisiana, and Texas are generally similar relying upon securitization through the private sector. In contrast, Mississippi's new law authorized a different securitization scheme by which the State, not a private-sector entity, will issue storm bonds and provide investors with "full faith and credit" guarantees. The transition to storm cost recovery via securitization represents an extraordinary relinquishment of future PSC regulatory authority and a shifting of all economic burdens associated with storm-recovery bonds from an IOU to its customers. Florida was the first of the four states to pass storm securitization legislation, and in July 2006, the Florida PSC was the first in the Nation to finalize a financing order allowing securitization of Florida Power & Light's storm costs for both the 2004 and 2005 seasons.

Researchers also discovered that federal grants have been appropriated to privately-owned utilities to offset energy infrastructure reconstruction costs. The U.S. Congress passed two FY 2006 emergency supplemental appropriations bills that provided $11.5 billion and $5.2 billion to the Community Development Block Grant (CDBG) program administered by the U.S. Department of Housing and Urban Development (HUD). Both statutes specifically state that an undefined portion of the total $16.7 billion appropriated can be used *(Continued on Page 13)*

**Securitization** *(Continued from Page 12)*
for "restoration of infrastructure." Researchers uncovered only two instances prior to FY 2006 where the Congress made emergency appropriations for CDBGs providing allocations to IOUs, both of which became mired in controversy.

All four Gulf Coast states examined by CIP Program researchers are using securitization as an option to pay for the costs of unprecedented electric infrastructure destruction. At least two of these states intend to use what appears to be a small percentage of their overall CDBG allocations to pay some of the IOUs' infrastructure recovery costs. Researchers' discussions with experts in the region revealed some concerns about over-reliance on securitization and HUD block grants as future storm recovery mechanisms.

The most frequently mentioned benefits of storm bonds with 10 to 15+ year maturities are that utilities receive a more immediate infusion of cash to pay for storm costs and that the "rate shock" to customers is minimized when compared to conventional methods such as 24- to 36-month "temporary" surcharges. Securitization insulates the utility from the issuance of debt because its customers, not it, are the debtors. This preserves the utility's credit position. AAA-rated bonds provide investors with security and ratepayers with "least cost" financing. Given the data and information currently available, these claimed benefits seem achievable. Yet independent ratings agencies and other experts caution that securitization can be overdone – it is not a panacea for each and every utility cost recovery docket. Ellen Lapson of Fitch Ratings, for example, suggests that any given securitized bond issue should be less than 20 percent of the total utility bill and preferably much less. She and other experts advise against using securitization to pay for fuel costs, retiring profit-earning assets, or to finance a "permanent layer of utility capital structure."

***"Over the longer term, securitization may fail if it is repeatedly used for the kinds of costs incurred today that reasonably could and should be paid for today; if it mortgages ratepayers for generations; or if the cumulative total costs of securitizations exceed what independent ratings firms and investors will endorse."***

Over the longer term, securitization may fail if it is repeatedly used for the kinds of costs incurred today that reasonably could and should be paid for today; if it mortgages ratepayers for generations; or if the cumulative total costs of securitizations exceed what independent ratings firms and investors will endorse. CIP Program researchers often posed hypothetical "what ifs" to experts interviewed for the project, such as "the financing order pays for the costs of year 2005 hurricanes over 12 years. What if securitization continues to be used for the next year's storms, the next, and the next?" The likelihood that the Gulf Coast states will escape one if not several costly disasters over the proposed life of today's storm recovery bonds seems remote.

Use of CDBGs for IOUs' storm recovery costs raises other questions for which there are no definitive answers at this time. When a regional catastrophe overwhelms the abilities of state emergency officials and IOUs to quickly and comprehensibly restore electricity without then sending ratepayers into a tailspin and thus retarding economic recovery and growth, a limited reliance on CDBG money may be acceptable public policy. If, however, commissions, utilities, and their customers develop a dependency on federal grants to avoid making tough but necessary choices about continued development in harm's way, and to avoid planning and paying for a hardened, more resilient electric power infrastructure, then ad hoc use of CDBG funds may come to be viewed as unwise. Determining the answer will depend on how fairly and effectively federal money is delivered, used, and accounted for. Implementation, accountability, and outcomes will matter.

CIP Program research to date suggests that a legal twilight zone exists between Stafford Act emergency authorities and a federal response to long-term infrastructure reconstruction needs that lie beyond Stafford. From the limited record, it is not clear that CDBGs, funded in the emotional and political contexts of national disasters and emergency supplementals, are the appropriate instrument to fill the void. ❖

## CIP Law Team attends ABA event featuring keynote speech by Assistant Secretary Paul McHale

Members of the CIP law team attended a breakfast hosted by the ABA's Standing Committee on Law and National Security on Friday, September 29, 2006. The featured speaker was Mr. Paul McHale, Assistant Secretary of Defense for Homeland Defense. Originally from Bethlehem, Pennsylvania, Secretary McHale served in the U.S. Marines and was a member of both the Pennsylvania House of Representatives and the United States House of Representatives. He was nominated to his current post by President George Bush on January 9, 2003 and was confirmed by the United States Senate on February 4, 2003.

The theme of Secretary McHale's talk was the role of the Department of Defense in homeland security, including the protection of critical infrastructure. He began with a discussion of the difference between the mandates of the Department of Defense (DOD) and that of the Department of Homeland Security (DHS). An important difference between the two involves the fact that while DHS looks to protect the United States through systems and procedures rooted in law enforcement, DOD's mandate involves systems and procedures rooted in military war-fighting.

Secretary McHale spoke of the need for the various agencies involved in protecting the United States homeland to effectively communicate amongst themselves. He made reference to the 1986 Goldwater-Nichols Act in which the military's operational authority was centralized through the Chairman of the Joint Chiefs as opposed to the service chiefs. The Act led to the coordination of policy amongst the various military branches rather than the development of individual policies within each branch which had contributed to an environment of inter-service rivalry and inefficiency.

Secretary McHale also spoke to the importance of the military remaining subordinate to civilian command, a cornerstone of the American system. For example, under the *posse comitatus* statute the United States military is prohibited from enforcing domestic law, except in certain prescribed conditions. Secretary McHale underlined the need to retain this civilian-military relationship, and made reference to its historical beginnings in the Federalist Papers writings of Alexander Hamilton.

For Hamilton, the main threat to be avoided is the dependency that can arise should a civilian government look to the military to secure its internal order. Hamilton feared that as soon as the government started deferring to the military, it would embark upon a path that would finally lead to a total reliance at the price of civil liberties.

Secretary McHale spoke for about one hour, including fielding questions. ❖

## October is National Cyber Security Awareness Month


Download "Protect Your Workplace" posters, a Cyber Security Toolkit, and more information on promoting cyber security at http://www.dhs.gov/xprevprot/programs/gc_1158611596104.shtm

**Oellrich** *(Continued from Page 10)*
this for a living 24x7. You can't have your CFO or your general counsel being responsible for all of the insurance decisions within your company.

MS. MESERVE: Harry, you have told us what you want. You want that data hidden somewhere in the bowels of government.

MR. OELLRICH: Right.

MS. MESERVE: Have you got an action plan? Have you got some specific concrete steps, ideas on how to grab hold of that and pull it out?

MR. OELLRICH: Well, I think the place that it really all starts from is by staying away from the trap that you can all fall into with many sectors and with many industries, and that is just saying "the insurance industry," or "the reinsurance industry." What you have in that space is an incredible diversity of different companies, different corporate cultures, different goals, different objectives. But what I think you'll find when you go out and talk to the senior executives of those companies, they all recognize that they are part of critical infrastructure themselves and that their goal is to be part of the solution as opposed to part of the problem.

And if you can tie into specific individuals that get certain issues, and be able to know that they have counterparts within government that can work certain issues with them, that is going to go a long way towards being able to get enough specificity to be able to maybe drill down and get at some of what we think is part of the answer. ❖

**Noznesky** *(Continued from Page 4)*
addressing specific plans with good, solid private sector input, good dialogue between the two.

***"So culturally, we know that those relationships with the state and local governments and the federal government are critical before a disaster. And if there's one thing that I could say ... is that in business continuity planning it is absolutely critical to develop those relationships and those dialogues before [a catastrophe]."***

There is the new implementation of the joint field operations, private sector liaison that DHS is going to implement – I think this is very critical because when there is a disaster, it is going to be very critical for that single point of contact, that one coordinator. And for the private sector, I think for all of the sectors in the private sector, I think this is going to be a positive.

The new Homeland Security Information Network, which is started over the last year, year-and-a-half, I think is going to be a positive to getting information out, situational awareness, perhaps early warning. And it's in its infancy, but I think that is an area that is going to continue to be strengthened.

Also, the Department of State many years ago created the Overseas Security Advisory Council, and that has been an outstanding public-private partnership, particularly for U.S. companies doing business overseas. There is an excellent exchange of information, threat information, which is critical to being able to do any kind of risk assessment and manage risk. And I think there is a real place for a domestic security advisory council for companies relating to the Department of Homeland Security or homeland security issues, and now that looks like it's beginning to take off. So I would like to see that as we move forward to develop and mature.

MS. MESERVE: You have mentioned a number of different things, and I wonder if there is room for confusion. Are there in some instances too many possible channels for information to flow that might muddy the picture for you?

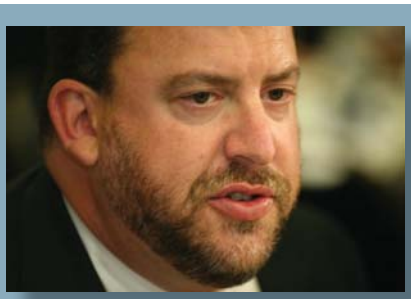
MR. NOZNESKY: It could. I do believe, though, that the Department of Homeland Security is trying to coordinate that information, and I think the HSIN, or the Homeland Security Information Network, should help to improve the coordination of information that comes out. We'll see. That is all a work in progress, but certainly that is a factor. ❖

**Eisner** *(Continued from Page 7)*

MS. MESERVE: Did it stifle improvisation in some respects? I mean, the Coast Guard has been lauded for going off on its own and saying, "plans be damned," we are going to go out and rescue lives. Were there other people who you think held back, didn't do what they might have seen needed to be done because they were afraid of not following that plan to the letter?

***"So it's really important to be able to operate both at that sort of planning-coordination level to maximize the chance that your plans are going to have an impact, but not create a culture where businesses or private citizens or government somehow believe that the plan itself is going to fix everything."***

MR. EISNER: Well, I think it was less about not following the plan to the letter and a lot of folks being insecure about who had the ability to say okay to something. And as soon as folks started worrying that we didn't know



who could say okay, then you had companies not able to provide their capacity. You had volunteers not able to get what they needed done, and you had mayors and folks on the ground not able to get people to give them a thumbs-up because no one knew well enough who could say okay.

I think that is one of the things we have got to get right. We left it a little bit this time to be a struggle between national and state control over some of the big questions. I think we will see the next National Response Plan be a little bit clearer and more prescriptive that in this kind of situation it will be a state call; in this kind of situation it will be a federal call.

MS. MESERVE: I was going to ask you about the rewrite of the plan. Are there some specific things you want to see in there?

MR. EISNER: Well, of course from a corporation's point of view, we have a pretty narrow focus; we are a signatory of the National Response Plan. We just want to make sure that we give as much capacity to particularly the Red Cross, the National Volunteer Organizations Active in Disasters, and corporation assets so that we can move even more people and more assets faster. We have got in the course of a year 35,000 participants in AmeriCorp, Senior Corps, and Vista into the Gulf. We think we could have done even better, and we think that we could have helped Catholic Charities and Red Cross and Salvation Army be even more effective.

And even though those are operating on what you might think of as a different side than critical infrastructure, when you are on the ground in these communities and you see the mayors making decisions, they are literally – they have got a pool of people, and they are making horrible choices about whether they are going to be focusing on getting the water going, or whether they are going to be taking care of a hospital crisis. So when you are able to get those kinds of people on the ground managing things, it frees up capacity to be able to make some of the critical infrastructure work. ❖

The CIP Program is directed by John A. McCarthy, a member of the faculty at George Mason University School of Law. The CIP Program works in conjunction with James Madison University and seeks to fully integrate the disciplines of law, policy, and technology for enhancing the security of cyber-networks, physical systems and economic processes supporting the nation's critical infrastructure. The CIP Program is funded by a grant from The National Institute of Standards and Technology (NIST).

***The CIP Report*** is published by Zeichner Risk Analytics, LLC (ZRA) on behalf of the CIP Program. ZRA is the leading provider of risk and security governance knowledge for senior business and government professionals. ZRA's vision is to be a consistent and reliable source of strategic and operational intelligence to support core business processes, functions, and assurance goals.

If you would like to be added to the distribution list for ***The CIP Report***, please click on this link:
http://listserv.gmu.edu/cgi-bin/wa?SUBED1=cipp-report-l&A=1