

Center for American Progress



SPECIAL PRESENTATION:

**“NEW STRATEGIES TO PROTECT AMERICA: A
MARKET-BASED APPROACH TO PRIVATE SECTOR
SECURITY.”**

MODERATOR:

**PHILIP J. (P. J.) CROWLEY, SENIOR FELLOW AND DIRECTOR
OF NATIONAL DEFENSE AND HOMELAND SECURITY, CENTER
FOR AMERICAN PROGRESS**

AUTHORS:

**ROBERT HOUSMAN, FOUNDER AND
PRINCIPAL, THE HOUSEMAN GROUP**

TIMOTHY C. OLSON, ADVISOR, CHESAPEAKE GREEN FUELS

SPEAKERS:

**JAMIE GORELICK, MEMBER OF THE 9/11 COMMISSION;
PARTNER, WILMER, CUTLER, PICKERING, HALE & DORR**

JOANNE RUTKOWSKI, PARTNER, BAKER BOTTS

**JOE WHITLEY, FORMER GENERAL COUNSEL,
DEPARTMENT OF HOMELAND SECURITY**

**12:30 PM – 2:00 PM
THURSDAY, JULY 27, 2006**

**TRANSCRIPT PROVIDED BY
DC TRANSCRIPTION & MEDIA REPURPOSING**

MR. PHILIP J. CROWLEY: Good afternoon, ladies and gentlemen, and welcome to the Center for American Progress. I'm P. J. Crowley. I'm a senior fellow here and I direct the Center's Homeland Security Program. We're happy to have you here to discuss a new report that the Center is putting out and I should salute not only one of the authors that is on the panel, Robert Housman, but one of the authors who stood for the bar yesterday and thought it was overload if he both had to defend himself before the bar and also defend his report on the same week. But, Timothy Olson, you must stand up and take a bow.

(Applause.)

MR. CROWLEY: Well, if you are taking the bar tomorrow, you have some pretty good advice and counsel here if you needed it. But there's an excellent report that we'll be discussing today on creating better market forces to encourage stronger security among the private sector.

Much has changed over five years since 9/11, but I think as one assessment – among that change, the private sector has arguably adapted least to this new security environment that we confront. And this is of obvious concern because the private sector operates 85 percent of the critical infrastructure in our society, which means they are very much at risk of the ongoing terrorism threat that we face in this country.

We know that there were recent plots unearthed in Toronto, Miami, and a plot from Lebanon involving the swamping of Manhattan. These plots may have been more aspirational than real, but they point out that the al Qaeda playbook and its affiliates' playbook has not changed over five years: they still wish to attack prominent structures, kill as many innocent civilians as possible, and exercise as much leverage as they can on the U.S. economy and U.S. policy.

And so confronted with a situation where progress is uneven, but many critical sectors of our economy are not adapting either enough or adapting fast enough to match this ongoing threat, the question is what we do about it? Markets can work. No one suggests that markets are perfect, and currently markets value efficiency more than security. And there's a perception that these two things are in conflict, but when you look from a social standpoint we have to find a way to eliminate that perception of conflict and change the current market dynamic.

And with this context, Rob Housman and Timothy Olson have proposed in their report that a market-based remedy using existing SEC authorities to improve private-sector reporting and, perhaps similar to what we have viewed under Sarbanes-Oxley, increased attention in corporate boardrooms to homeland security. I think it's important to point out that this is not necessarily a remedy in and of itself, but could be one tool that

could be exercised to prompt the private sector to do more to protect critical infrastructure, supply chains, and other vital elements of the U.S. economy.

In addition to our two authors, we have an expert panel here to comment on the proposal and help us evaluate, almost five years after 9/11, the state of private sector security and what can be done or should be done to improve security with a greater sense of purpose and urgency as we approach the fifth anniversary of 9/11.

So to introduce very briefly our panelists, to my immediate left Jamie Gorelick, member of the 9/11 Commission and now a partner at a prominent law firm here in Washington, D.C. To her left Joanne Rutkowski a partner at Baker Botts and a former member of the SEC. Also we have Joe Whitley, former general counsel for the Department of Homeland Security.

One brief caution here is that if you haven't turned off your cell phones already, please do so. And I also before we start want to – any time we do an event here at the center for American Progress it takes great teamwork and I wish to salute Anna Soellner, Antoine Morris, Adorna Williams, Trevor Kincaid, Alex Pryor, Mira Patel and Josh Cox (sp) for all of their help in helping put this event together. With that, we'll start off with Robert Housman giving us a brief summary of the report. Each of you has a copy of the report at your chair.

MR. ROBERT HOUSMAN: Thanks, P. J., and let me thank P. J. and the other people here at the Center for all the support they've given us in this process and also all the people who were kind enough to give their time in reviewing it and helping us hone arguments and fix problems.

Let me start with the purposes of the report – why we did this. We wanted to examine the application of SEC disclosure rules in the area of homeland security and then, assuming they did apply, we wanted to determine the degree of compliance. Second, we wanted to examine the use of SEC disclosure rules as a market-based mechanism for homeland security.

Why did we focus on the SEC rules? Well, a number of reasons. First and foremost the rules already exist which in this political climate has immense political and policy advantages. Second, as we looked at the rules it was our first conclusion that the rules already required disclosure of material information and that includes homeland security information in a number of areas. Additionally, the authors – we believed that there was value beyond just the disclosure you see on the paper – that one of the benefits of an SEC disclosure regime is that it forces or compels or encourages companies to inculcate values into their operations, and in this case inculcate security, and it engages senior management and the data shows that where senior management is engaged on these issues security improves. Additionally it was our conclusion that the current practice created market failures that actually worked to the detriment of both national security, investor security, and actually to these companies over the long term as well.

And lastly, market-based measures have a number of advantages. They obviously have disadvantages including the vagaries of markets, but there are a number of advantages to market-based measures that made them appealing to look at. Let me say, though, while highly advantageous, market-based measures for homeland security are not nor should they be viewed as a silver bullet. In some instances – perhaps many instances – the threat or risk is such that greater surety and certainty is required. However, even in those cases there’s an appeal to linking those or using those other types of policy interventions alongside market-based measures as well.

Now, let me turn to the rules that we focused on. These rules come by way of the 33 and 34 acts in regulation SK. This is all described in painful detail in the report, particularly the long version, and I won’t bore you with it. But item 101 requires a description of the business – a narrative form description of the business. Suffice it to say, if there are inherent risks in what you do, those sorts of risks need to be disclosed to the investor whether you’re relying upon a single supplier of a raw material or whether you have a single customer; for example, maybe you’re single biggest consumer – at the end of the day the one that you’re most dependant upon is a Wal-Mart and if their supply chain breaks, your customer vanishes and you’re at risk.

Item 103 requires disclosure of legal proceedings. Any material pending legal proceeding other than normal a routine litigation; this includes agency proceedings so, for example, if the Coast Guard has begun an enforcement action against a company for violation of the Maritime Transportation Security Act, investors should know about it. Even contemplated proceedings need to be disclosed so, for example, if DHS is looking in to potential violations of money laundering statutes or rules, those sorts of things also should be disclosed. Item 303 – the management discussion and analysis – you are required to provide a historical perspective summary of the opportunities and risks your company faces, focusing on changes to operations. Here, for example, if there is a new homeland security law that’s going to force you to adopt new technologies or change your manufacturing processes, arguably that should be disclosed. And trends and uncertainties – in fact, one could argue that the trend in terrorism and the uncertainties of liabilities around terrorism as a whole are trends and uncertainties that would fall within the MD&A requirement. You can see here the hot-button issues that the SEC has of late described as what they’re focused on in MD&A and it’s obvious that a number of them have direct application in the area of homeland security.

Those are the rules. How are we doing? What does it look like out there? What’s the current practice? Tim and I analyzed over 40 companies. I should say that we analyzed literally hundreds on companies; we specifically focused on 40 companies in a range of sectors. We tried to be broad across critical infrastructures ranging from nuclear power to IT to food service and retail. What we found was the actual application of the provisions to homeland security matters is little understood and less followed; current disclosures vary widely in terms of both quantity and quality, and that occurs both across and within sectors.

Few companies substantively disclosed homeland security matters. Where disclosures were made, they were generally inadequate for shareholder purposes. And interestingly – and these are the two things I thought were most interesting: first, by and large no disclosure addressed comparative or competitive advantages or disadvantages by virtue of security policies or programs; and no disclosures discussed what you might call control measures. We would call them security. What do you do to offset the risk to your operations? And I think that actually hurts companies in the long run because many companies have changed, particularly sort of forward looking companies. Companies most at risk have changed what they're doing and while many people may know of the risks to these companies, few people know about what they're doing to address those risks. Lastly, there's very little homeland security in securities these days.

Now, let me turn to some specific examples that illustrate these points. The chemical industry – companies face potentially enormous liabilities in the case of an attack on one of their facilities. Many of these companies already face new security rules. They face the likelihood of even more security legislation, which is currently pending in the Congress that would have a material impact on their operations. None of the publicly trading companies within this sector that were considered or perceived by many as most at risk substantively addressed these issues; only three even alluded to the threat.

Example two is the Disney Company. It's an iconic company heavily identified with American culture; that puts it square in the crosshairs of the terrorists. The risks to the company were perceived by both the company and DHS sufficient to justify no-fly restrictions over Disney's theme parks. That puts it on par with nuclear sub bases, chemical weapons facilities, the White House, and the ranch at Crawford. Its cruise operations are under the MTSA. Its food service operations fall under a new food security guidance. Suffice it to say, it's got lot of homeland security regulation that it's looking at. However, Disney's form 10K makes no mention of terrorism, no mention of homeland security, and no mention of what it's doing about these risks.

Example three: Entergy nuclear power. There are still serious questions about the security at our nuclear plants. Entergy operates a controversial, high-risk plant at Indian Point just north of New York City. A 2002 study commissioned by the company itself found that 81 percent of its facility's guard force believed that it could not adequately defend the plant. And you can see the worst-case scenario estimates are very large and clearly material. Yet the 10K makes only one mention of terrorism within a long laundry list of potential concerns, it provided no substantive discussion of their threat or its security, and it made only one mention of a federally mandate insurance plan that covers the nuclear industry.

Example four is the insurance industry. The insurance industry suffered massive losses post 9/11 and required federal legislation to arguably save it. I want to focus on two companies here because I think they're illustrative: Aeon, its 10K makes no mention of the risk of terrorism, it made no mention of the potential impact of TRIA non renewal in pre 2005. TRIA is the Terrorism Risk Insurance Act: the federal backstop. Its lifespan

was closing in 2005 and there was a serious question about whether or not it will be extended. During this timeframe, Aeon did not talk about the risk of non-renewal for its shareholders; however, in lobbying Congress Aeon said the private insurance market cannot operate without some form of public backstop.

That seems material to me. Post the renewal of TRIA, there was no mention of the fact that in 2007 we'll be looking at renewing or not renewing TRIA again and that will be a major challenge.

Marsh McLennan is one of the examples I really like. Marsh owns Kroll which is one of the largest security companies, very reputable, very good security firm. The CEO of Marsh is the former CEO of Kroll and the CEO has long been saying – and I would completely agree with this statement – before Fortune 500 clients that there will likely be a terrorist attack against them both at home or abroad for the foreseeable future. That's what they've been telling their clients; however, what they've been telling their shareholders is one laundry list mention of the threat of terrorism and no discussion of TRIA. That seems to me incongruent.

Let me step back from these examples and say on a macro-scale what observations are there. I would offer three. One, that a significant amount of information that is arguably or on its face material – of homeland security information that's on its face material is not being disclosed and arguably should be being disclosed. Second, that this wide variation in disclosures creates in fact a market disincentive to forward-looking companies that want to do more in their security and also want to exercise greater candor with the investing public. Think of it this way: if you talk about your security, even if you're doing the best job in the world, if your competitor who is probably not doing as much as you are doesn't mention the issue at all, even saying all the good things you have to say you probably look worse and you will scare off investors or at least reasonable investors.

Lastly, it seems to us that we are squandering an enormous opportunity to use an existing tool that while not a silver bullet can significantly advance homeland security within the critical infrastructure companies of the United States. If you wanted to seize that opportunity, we offer up a number of options for SEC action to do so. The first is the bully pulpit: simply getting out there and raising these issues with the publicly traded companies. The second would be to review specific filings and issue comment letters. The third would be interpretive guidance: here's what the current rules are and here's how we see security fitting in to it. The fourth, and not my favorite at this time, is enforcement actions. The fifth would be for the SEC to say, we think security is very important but we don't think the current rules do it justice or don't fit well and because of that we're going to issue new rules to cover security disclosures. This would be akin to what the commission has done in the area of the environment.

I would suggest that this is an extraordinary opportunity for Chairman Cox to put his imprint on the SEC and markets. Many of you know that Chairman Cox recently was

the chair of the Homeland Security Committee in the House, so he's very aware of these issues and obviously concerned.

What should not be disclosed? We offer up a list of general areas where we think material information should be disclosed with respect to security. Let me stress a few point, though. Disclosure should be strategic, not tactical, that way we don't provide the terrorists a roadmap. Classified information obviously should not be disclosed. One could argue even sensitive information should not be disclosed. Judgment calls will require agency input and by that I mean both the SEC, DHS, and others.

The other aspect to SEC compliance is the watchword of today's Sarbanes-Oxley – SOX. Sarbanes-Oxley requires companies to have internal controls to ensure full and accurate reporting. Material event and contingent liability disclosure requirements are also there, and it personalizes all of this so that management must take a significant role in it. What does SOX require in the area of homeland security? The short answer is no one fully knows yet, but I think these are the types of things that we think a forward-looking company should be looking at in terms of SOX compliance in the area of security.

Lastly, we touch on a number of other issues that I don't want to have lost in the mix. First, the need for better government and industry cooperation – information sharing. Industry has a good beef with the government that it's not getting the information it needs. Interestingly, one of the expert reviewers that we used on this said that they thought a disclosure regime might actually force the government's hand to be a better partner in this way. We also stressed the need for audit shield protections. If you want companies to proactively audit their operations and take steps to fix problems, audit shield protections probably should be looked at.

While we were doing this, we were in the midst of foreign ownership issues with respect to the Dubai Ports. One of the interesting things – and I don't think here, again, it's a silver bullet, but one of the interesting things is many of the foreign companies – owners of large critical infrastructure also report under the SEC rules as foreign registrants. And I think that this is an interesting nondiscriminatory way for the American public and the investing public to have a better sense of what the security is at these operations of foreign companies with respect to domestic critical infrastructure. And with that, I will turn it over to the panel.

MR. CROWLEY: Joanne, you've served at the SEC. Could this work?

MS. JOANNE RUTKOWSKI: I think it could. I'd like to talk a little bit about the framework under existing law and really when we were putting this together, we were thinking about materiality and disclosure not so much as the impact on the markets the way disclosure of a competitive issue, but really as a way of modifying behavior. And certainly disclosure is a time honored tool for encouraging certain actions, discouraging others.

If you look at the current law, basically a company is required to disclose material events, material items. Part of the problem I think currently is that – what is material and how does it apply in this situation? The report points out very well that for many industries just if you're looking at the likelihood of a terrorist event weighed against the magnitude it probably doesn't become a material event. Certainly, though, for these strategic industries this is an important issue and one that could be considered.

When you think about disclosure as a way of modifying behavior, certainly SOX 404 come to mind. The work that the companies have done over the past couple of years putting those controls in place and assessing them; at a minimum, for example, management has paid a lot more attention to the security of information systems.

Considering a proactive approach to terrorism and disclosure, there is an analogy to what the SEC did with Y2K. Back in 1998 anticipating the problem, the SEC issued an interpretative release – not a rule. And in it they basically encouraged the companies to provide disclosure on four points, the company's assessment of the situation vis-à-vis Y2K, the budget or the estimated cost of dealing with it, the risks that they saw; and very importantly the effect of those risks on their material relationships, say, with vendors and customers; and finally, the existence or not of a contingency plan.

So there is a model that could be used. I think the difference is it's not a perfect analogy because you're obviously – with Y2K you were headed towards one point in time: there was a very discreet target. Here, as the report points out, there really isn't a definition of security across the board. Terrorism could be anywhere or nowhere. That's an issue that needs to be explored and so I thought that basically those four categories that the SEC used I think would be a good starting point to capture some of the thoughts that you have laid out in the report.

Just some general thoughts. One is when I think about the terrorism and preparing for the next event, I guess it's sort of like the company is preparing for the next Katrina. It's almost inevitable that it's going to happen, but how and where? And so there is some experience, I think, in companies for that kind of planning. The fact that disclosure would be mandatory or could be mandatory, could be required doesn't mean that you're providing a roadmap for terrorists. Companies have oodles of experience on a day-to-day basis dealing with identifying material risks and telling the world how they're going to deal with them and manage to do this without disclosing competitive secrets.

That said, if you are going to a disclosure regime, I think it will be very necessary to ensure heightened protection for any confidential information that is provided to the SEC and that may mean enhanced FOIA protection.

Finally, I think if companies are in good faith trying to comply and disclosing, that you need to protect them if somewhere down the road the system fails. And currently you do have the statutory safe harbors for forward-looking statements which most of your security preparation would be as long as it's accompanied by meaningful disclosure. So that will give you some protection in the private policies but it's definitely

something you should not penalize the company for trying to take the right steps. So I thought the report was excellent and it certainly is thought provoking. More work needs to be done and I guess the question is this one of a (unintelligible) of tools, is this the best way, or is this the only way.

Thank you.

MR. CROWLEY: Joe, you were at DHS at the outset of the department. When the administration has looked at critical infrastructure, it has put a great deal of faith in markets and perhaps the current debate over chemical security is at least one example where that faith has not necessarily seen a return. What is your sense of this and is this a way to spur the markets to do more or do the companies do more through market behavior?

MR. JOE WHITLEY: Thanks, P. J., and thanks for the invitation to be here today to speak with this group at the Center for American Progress and thanks to everybody who put this together. I want to join in the applause for Rob Housman and Tim Olson on this report. I think it's an excellent and thought provoking document. I commend it to your reading. Don't read it too late at night because you'll be sound asleep, but it's quite lengthy and –

MS. RUTKOWSKI: We thought you were going to talk about nightmares.

MR. WHITLEY: No. Well, the examples in it would keep you awake at night. Some of them might, but with my advanced case of narcolepsy I can sleep through anything. In any event, I do think it's important to look at how the department has addressed these issues and P. J. neatly set up an opportunity for me to talk about the Department of Homeland Security.

The Department of Homeland Security is 22 different agencies that came together. Everybody's heard this before – 180,000 people. Some new parts were created, there were some of the old parts that you all know about probably: Customs, Immigration, Secret Service, FEMA, all within this new department, but a look at infrastructure was one of the critical pieces that was in the Homeland Security Act for 2002.

In addition to that I'll look at intelligence sharing, information sharing, so those two really run together. And sitting to my right is probably one of the world's leading experts on the Department of Homeland Security, at least looking at it through the eyes of the 9/11 Commission, so I look forward to hearing what Jamie Gorelick has to say in a moment. So every day there was an opportunity to build this new framework. We had an undersecretary dealing with infrastructure and information together, all combined.

And the notion was – in this new framework in terms of legislation was a voluntary approach. You hear this said over and over again in fact and in Tim and Rob's book, they talk about how 85 percent of America's infrastructure is held in private hands,

and that is what drives this discussion here today. So the notion was that the Department of Homeland Security would reach out to that infrastructure through some sector-specific committees and organizations to work with those sectors. This is all laid out in some of the documents that you can find that Homeland Security has generated, most recently the National Infrastructure Protection Plan, otherwise known by the acronym NIPP, which is guided by the Homeland Security presidential directive seven, which really puts in play a different regime – a more proactive regime looking at the different sectors in our economy to include things like telecommunications, obviously, water purification systems, chemical plants – all that falls within a sector.

But as you look at a department and you describe this department as really developmental almost, you think about well how does an infant develop? Well, at first there are not a lot of teeth for the infant to chew on its food so it has to eat something softer in effect. When Congress created this new department, they created a department that was going to have to operate on an encouragement model almost. And I do think that there are a lot of great industries in the United States, tremendous motivation in the boardrooms to do the right thing, but also a split personality exists in those board rooms about how do we achieve profitability. And if you're competitors, if you're in a supply chain and one of those competitors in the chain decides to do the right thing and the other nine don't and there is not an event, where is the benefit? And I think that's one of the challenges that you have sort of in real-world terms looking at this issue.

The boardroom is where all this begins and ends and I think that in Rob and Tim's report they do look at this issue in extreme detail. I don't think anyone's really looked at it. In the boardroom, though, they are looking for metrics. How do they measure whether something's been valuable to their shareholders? And I don't think that homeland security is necessarily an area that has metrics associated with it. Chemical plants – transportation of hazardous material is an area that we can see in the safety environment, safety and security – the twins if you will – that look at these issues, environmental enforcement has looked at safety over the years and there are teeth, if you will, in the environmental enforcement aspect of this and also SEC oversight of whether or not you have the right things in place.

I don't want to go on too long because I really want to hear the other panelists today and hear what they have to say, but I have come to the conclusion not just influenced by this report but I have come to the conclusion that it would be useful, and it's my hope that the SEC will look at this report and will have an opportunity for Chairman Cox to assess it and give us feedback.

The department is moving downfield. At the same time, I think that if you look at the department it really is an outreach organization built on the notion that it's a partner not only with its federal cabinet agencies that it works with, but also with the private sector. And I think that there's a way to develop metrics when you look at consequence, vulnerability, and threat as you look at where a plant is located, the facility is located. So we need to think of metrics to give industry a way to work its way out of these issues.

I was telling P. J. earlier, and then I'll end, that this really is a program that should be almost a day long. You can't capture it in this hour. Nonetheless, if you haven't read it, I commend you reading the report that Bob and Tim have put together. It's just outstanding. Thank you very much.

MR. CROWLEY: Jamie, you are almost in a unique position. You're now at Wilmer Cutler, before that the 9/11 Commission, before that the Justice Department, before that Defense Department. Particularly while on the 9/11 Commission, the commission focused a great deal on the difficulty of sharing information, getting the right information in the right place at the right time. This at least is an attempt to put more information out in the public sphere and also improve perspective for government officials who have to evaluate how to get the private sector to do what it needs to do. How do you see this?

MS. JAMIE GORELICK: Well the other perspective that I bring to this is the President's Commission on Critical Infrastructure Protection, where we – and these are conversations that have been going on within the government now for over 10 years about how to get the private sector engaged. So let me say first that I think the goal is very important. I mean, there's no question that getting the private sector engaged is a critical factor in making the country safer. And the notion of using market-based incentives is also a very good one. So let me talk about from my perspective as a corporate board member and as a counselor to companies where I think the private sector is, although obviously one can only generalize in the short period that we have. And then talk about what the mechanisms currently are and whether this would add or subtract from that.

Surely companies have in place plans to protect their own physical plant and their own IT and communications infrastructure. That is a pretty basic requirement for most companies today and I think it is embraced by companies. What are the mechanisms for incenting the right behaviors? Well, the first is self-interest. As I do, if you have your office in the CitiGroup Building, you notice lots more security, control of entrance to the firm, entrance to the building, barriers, et cetera, and lots and lots of companies have done things like that.

Second, we haven't talked at all about the insurance industry and this is the insurance industry's job to assess risk and to put a price tag on it for their customers. If you have a risk that you could mitigate and you don't, you're going to pay a higher premium than if you do. And the insurance companies, seeing across industries, can look at what those risks are and can put a number on them – maybe not a hugely accurate number, but it can make a better stab at it than any individual company can. And it can – because it charges premiums, it has a regular conversation with its customers about the cost of doing X versus Y and the risk of not doing X versus Y. So I think the insurance industry brings to bear a tremendous amount of expertise and it is an overlooked element of the response of industry to Y2K. To be sure, the SEC did its part. To be sure, the Clinton administration was very energized in reaching out to the private sector.

But the insurance industry also said this is a big risk: if you want to be insured against this risk, there are certain things you have to do. Let's have a dialogue about what you're doing. Let's talk about best practices. And pretty soon this was really in the boardrooms before the CEOs and was part of an enormous and very costly corporate effort.

So the third mechanism Joe touched on some is industry groups. It's my perception that if there is an industry standard for something and your company is not meeting that standard there is going to be a discussion in the boardroom and at the highest corporate levels about why you're not meeting that standard. So the question is where are the standards? How do you get those standards in place? As Joe said, and I think very accurately, the Department of Homeland Security and the federal government generally had and put almost no teeth into the process of bringing together industry groups because, as he noted, industry was to say the least ambivalent. On the one hand they wanted help, on the other hand they didn't want interference – a very fine line between those two modes of government interaction.

So what you have is a system in which we've said to various industry groupings, go off and do good. Go do the right thing. And so almost as volunteers they have come together to try to set standards and share information. My own personal view, and I've had this view since 1995 when we started the critical infrastructure effort, is that government actually needs to play a role in bringing industry groups together, and it is more of a help to industry than a harm. It is an act against nature for competitors to sit together and share their vulnerabilities; it's just not done. So if you have a governmental entity that houses a group, that prompts questions, that can share intelligence about threats, that can come up with the metrics by which one as a responsible corporate citizen would measure risk, that's a big help. And if the industry groups themselves or the government or some combination promulgates standards, then even if there's no enforcement mechanism, that will be self-enforcing because if you hadn't made a standard and a bad thing happens guess who shows up? Plaintiff's lawyers – bad thing.

So you want to know what the standards are and you want to know if you're meeting them. So to me that's the most bang for your buck that you could get. Now where does a proposal like this come in and where can it play a role? I come down on both sides of the question, is this a good thing? I come down favorably toward the notion of, as Joanne put it, using the bully pulpit. It does seem to me that the people who write these disclosures, many of whom are my wonderful securities partners at Wilmer Hale, need to know that there are material risks or possibly material risks that need to be addressed as part of the list of things that you go down when you're thinking about materiality.

Materiality, as Joanne points out, is a very elastic term and when you have a low-probability, high-cost event and if nobody is telling you what the probability is, it's very easy to say we're in no different position than anybody else in the country so really there's not much for us to disclose here. I think the report does a good job of identifying exceptions to that general rule and industries where there may be a greater need for

attention to this issue. And that's where I think an engagement by the SEC to give some examples, to use the bully pulpit to energize the securities (unintelligible) which, after all, is reasonably small and reasonably cohesive and when it gets seized with an issue it tends to do something about it, would be useful.

On the other hand, I would not be inclined to something more prescriptive. We have a history of political forces saying to the SEC, use your mechanisms to achieve my goal: I want full disclosure of every company that gives to Planned Parenthood. I want disclosure of every company's glass ceiling policies. I want disclosure – the most recent one is – of where company does business with an embargoed country and what the risks are. If you read the disclosures that have come out of that program, they are by and large useless in my personal view. There's a lot of gobbledygook, nobody knows what the standards are, it's too vague and so it's a lot of effort for not a lot of product except that somebody can say I told the SEC to do it. I just don't like social engineering through the securities rules and I'm sure, Joanne, you as a practitioner would agree with me. And I don't really feel that what you get out of that is a market-based solution. It's a politically based solution; it doesn't really inform an investor. I have not seen any investor activity move based upon a disclosure of business being done in embargoed countries and the risks coming out of that.

So I would say this is a very good contribution to the debate. I would say that there are other market-based mechanisms which we maybe should look at also, and that if we could encourage the SEC to have a dialogue on these issues informed by folks at the Department of Homeland security and elsewhere about what the risks are.

My last point is this is not an area of expertise of securities lawyers. They don't know where the risks are. They don't have access to that intelligence. Frankly, I don't think we should give it them, but we should help them develop some notion of who is at risk. I think that is actually a very powerful contribution.

MR. CROWLEY: I'm not sure the insurance industry has that kind of expertise either, but that's a separate conversation. Here's back to the panel and if we are currently in a situation where the market gets you this far in terms of a baseline of security, probably would be individually based on a company by company basis, and you see in certain areas that there is a social requirement – a societal requirement that is higher than that. Jamie, what you're saying the government has got to fill that gap.

MS. GORELICK: The government has to fill the information gap. The government is the one that knows what the threats are. It's done a threat assessment to the chemical industry. It's done a threat assessment of the critical nodes in our transportation infrastructure. It's done a lot of that. And to launch the SEC or Joanne as she's sitting doing the disclosure for a major American company into a process trying to figure out what the risks are absent that is impossible.

MR. CROWLEY: Does that get you to something of either a formal regulatory scheme of some fashion that gets you standards? I mean, if market forces aren't the

answer, then that leads you towards some sort of mandate whether it's just setting a clear bar and expecting industry in some fashion –

MS. GORELICK: If it were me – and I have been saying this for 10 years – I would have the government be much more supportive and invested in these industry groups, so I'll give you an example. The communications infrastructure is an exception to the rule. Its industry group is housed in something called NSTAC, which is at the Defense Department. The senior people within each of the companies have security clearances, they get briefings on what the risks are, and they actually come up with standards that they need to meet with interoperability concerns. They talk about and rehearse what they will do in the instance of various bad scenarios, whereas the other sectors don't profit from something like that. They literally pass the hat to stand up some group themselves.

I just think if you look at it, you're not going to get that sort of robust standard setting informed by the kind of information you need to be informed by by the incredible hands approach that we have. Now, both the Clinton and Bush administrations took this hands off approach. This is not a political problem. This is industry doesn't want this, we shouldn't do it. My guess is that that's really not right and industry could use help as long as it's assured that it's not intrusive and directive of how to conduct their business.

MS. RUTKOWSKI: Jamie, what's the background of the communications group?

MS. GORELICK: It's old. In other words it – yes, this is born of a statute decades and decades ago because there was an appreciation that some disaster – not necessarily a terrorist disaster, but some disaster could bring down serially the communications infrastructure of the United States. And the Defense Department, which is the most truly operational arm of the federal government, said we can't have that happen because we in order to defend the country need an operational communications infrastructure and it reached out to the communications industry. And if it were me, I would do the same thing in transportation and banking, et cetera.

MR. CROWLEY: Back down the panel in terms of reaction to what's been said here so far? And I suppose that's a good idea in theory, but when you go sector by sector there's not necessarily the same kind of industry cohesion that may exist in one. It may exist in one because there's a common purpose, but it may be more competitive depending on which if the 17 sectors of critical resource areas we're talking about. Right?

MR. HOUSMAN: I think that's right. I actually like the idea. I think Jamie's idea has immense merit. I think the difficulty is severalfold. One is that I forget how you stated it, but I liked this sort of natural aversion. You stated it more strongly – a natural –

MS. GORELICK: I said it was an act against nature.

MR. HOUSMAN: An act against nature. (Laughter.) Thank you. I may steal from you with your permission – an act against nature for competitors to speak. In the communications industry, there is a more common purpose. If I have Sprint and you have Verizon, it's in both their interest that my firm speaks to your firm and so there's a natural reliance upon competitors to compete, but also to be able to work together as a communications web. In some other industries that sort of cohesion doesn't exist. I think that's a good point.

I also happen to like the notion of industry standards and actually I think industry standards play very well with a market-based mechanism like an SEC disclosure. It means it gives you a target to shoot at and I think that works very well.

I also agree with you: I would prefer not to see this as a necessarily individually prescriptive regime. I think the current rules actually provide what they need. I think nobody knows they have to do it.

MR. CROWLEY: I think, Joe, you mentioned the NIPP. Before the NIPP, there were the ISOCs (ph) and now there are the sector councils. What is DHS's experience in terms of the ability of the individual critical sectors to actually do this kind of cooperation and work cooperatively with the government to set these kind of informal rather than more prescriptive standards?

MR. WHITLEY: It's my observation that it's uneven. Speaking about the chemical industry they have taken a new approach with the American Chemistry Council and have advocated legislation on the Hill recently. I know you may have testified regarding that legislation, P. J. There are other parts of the other sector councils that were not as robust. I mean, telecommunications is the most robust part of the sector councils.

I think you can hold over people's heads the fear of another event only so long and people will go back to doing what they're doing. But having been at the Homeland Security and having been there and seen the rules we operated within, which many were congressionally mandated – some of which we great rules some of which were otherwise – I think the risk that industry runs by not being proactive – and I think this is the pitch – is that operate through your associations.

Transportation, for example. I think railroads – we've talked about this earlier – are moving a little more aggressively as a group even though they are competitors for rail lines to deal with the issues associated with the movement of chlorine, for example. We can talk more about that in a minute. But I think that the worst-case scenario – and I respect that the 535 people that reside at the other end of Washington – would be some quickly passed piece of legislation to put in place a statutory regime that deals with every industry in America in all the different sectors. There's no real template for every different sector and I think that the opportunity of a sector-specific council hopefully under any leadership – and I think Jamie is right: this is all really outside of the political

bailiwick. It really is about how can we preserve the economic engine that drives America. And Robert points that out in his materials.

I think it's critical that we see a joinder, and I think the department is moving toward a new regime, P. J., where the sector coordinating councils would have companion government coordinating councils and then there will be a cross-sector merger of that information, hopefully in what is called a partnership for critical information security, and then a whole world of new acronyms that I can wow you with called a PCIS, but I think the sharing of information between people in the sectors about their vulnerabilities is essential to effective defense of those companies and businesses. And I think the choices are clear and I think the opportunity to do something that's more economically based, more market-based is a good compromise.

In our society if you look at chemical plants – and I'll end on this – there are the Dows and DuPonts and the major companies that are aggressively working to protect their facilities. Then you have what is the lifeblood of American innovation: you have smaller companies, start-up companies that may not be able to go to the expenditure that some of the larger companies might be engaging in. So the challenge is – and I think Congress is trying to address this – in the fullness of time in how many legislative days we have remaining this year to pass some legislation dealing with it, and the *New York Times* I think editorialized on this this morning. The opportunity is now to do something about it and I think – P. J., I'll end on this note – if we can take – if Congress operates on a baby-step model in terms of oversight and suggesting regulation, it would be good. I think if we go too far, it will further push offshore U.S. industry to other countries.

MR. CROWLEY: Joanne, put your SEC hat on for a second here. Let's go the other end of the equation. If you are an investor, how do you find out – absent better disclosure on risk and what individual publicly traded companies are doing, how do you find out if a company has decided for one reason or another to bet the ranch that they're not going to be attacked?

MS. RUTKOWSKI: My background is mostly utilities, so I probably go to page three of the *Wall Street Journal*. (Laughter.) It's an important issue. That's a very good point and I just don't know what the answer is. One thing, though, with this whole disclosure exercise is I do think that it will have more focus on actually changing the behavior of the companies than perhaps informing the market. You made the point about the embargoed type countries. You're going to get disclosure that's very broad, very guarded; it may not address the question you're asking.

MR. CROWLEY: One last question for the panel before we open it up to the floor for questions. Businesses value certainty and what – since we've got lawyers at the table, what is the role of liability as being one of those incentives you're talking about? If you look back in the post-9/11 situation where they passed the Airline Transportation Bill and passed the victims compensation rule and it puts caps on certain liability of companies, is there a role here for liability in terms of saying to whatever mechanism to work into industry to say, look, we are going to set a very clear standard and then in

return for that standard if you meet it and you're able to certify it in some way, perhaps through annual security audits – whatever, just like we have financial audits – is the role for liability to be that incentive to say if you meet this standard and measurably reduce our vulnerability to terrorism that then there should be some sort of consideration of a cap on liabilities? Is that the kind of market-based incentive also that perhaps corporate America would respond to?

MS. GORELICK: You don't need actually to do any of that if you have standards. In other words, if the standards evolve and they're set particularly by agreement among the companies pursuant to what used to be ISACS are now the sector-specific councils – if they come up with standards or if the government issues them and you buy by the standards, as a practical matter you're not going to need to worry about liability because you will have been shown to be reasonable.

But the problem that industry faces, as you've heard, is that industry likes to minimize risk – is that they don't know what the standards, so you're left as a board member asking questions about what the best practices are; sometimes getting very definite answers, sometimes not. And I don't think that's a very satisfactory circumstance for either the companies or the country.

MR. CROWLEY: Which leads to a stronger role for DHS. On the one hand, at least up until now it appears in many cases it's been reticent to walk into and intrude into markets but what Jamie is basically saying is DHS has to make sure that whether it's prescriptive or whether it's by agreement, there have to be clear standards on what it will take.

MS. GORELICK: Could I just say – because I am not suggesting that DHS or anyone else actually makes standards for industry, but rather create an environment with antitrust immunity and all the other – FOIA immunity and all the others things that you need there to allow industry participants to talk to each other in a meaningful way, for such standards to develop informed by such intelligence as the government can share.

MS. RUTKOWSKI: P. J., to go back to your point, I was thinking about the nuclear industry and (unintelligible), which is their mutual insurance company self-insurance, and maybe that's the answer. It's the industry group. Obviously, they're setting standards. You're reducing liability because you have to adhere to those standards or face the liability. And as you pointed out in your report, the disclosure concerning (unintelligible) participation is pretty cursory. So if you were asking – and maybe that's the answer to your question – we thought about this and –

MR. HOUSMAN: P. J., if I may, I do think that Jamie, you're a bit of a unique board member. I've had a fair amount of experience with other boards advising corporate leadership and quite frankly I think – and if you look at the research, the actual metrics on it, most corporate leadership is not as engaged as you are. In fact, most corporate leadership hasn't met with their CSO over the last year. They just haven't sat

down with this individual and said tell me how I'm doing. Most boards have not called the CSO in and I think that's a serious risk.

The other thing I do think, P. J., to answer your question directly is there is a role for liability and one of the things that I think is interesting about liability and market mechanisms versus standards, and I also like the interplay by the way, standards tend to be fix birds and you know what you shoot at, but that means that they exist in a point in time that's fixed and they're knowable. They tend to focus on the four Gs – guards, guns, gates and gadgets – and so they're not living, breathing organisms and they don't tend to evolve. Once you've done it, you kind of do it and you say, "Thank God I've got that done."

I think one of the nice things about market mechanisms is that the market self-polices itself and drives the bar to the moment. The other thing with liability is liability also self-polices itself in the sense of the reasonable man. The reasonable man is different today than he was before 9/11, and that's a big change. Now who is that reasonable man? I don't know, but I know he is different than he was before 9/11.

MS. GORELICK: The reasonable man is also different after 9/11 because after 9/11 we were told no one would invest in certain kinds of real estate and therefore we needed a massive insurance program. Well, you know since we haven't had an attack, people are back investing without regard to insurance.

MR. HOUSMAN: Well, and I think actually that program may in fact be an enormous disincentive to risk integration because if you know have a backstop – the sort of insurance mechanisms you've been talk about – you don't have to worry necessarily as much.

MR. WHITLEY: Just a word or two. This could go on, as we say, all day, but I wanted to comment on P. J.'s question to us. I do think there are a couple of things that we should just take note of. One is the Safety Act, which is actually in the Homeland Security Act, which creates some litigation safe harbor, if you will, for the developers of antiterrorism technology. And it can be designated and certified under that process and get some relief – limitations on your damages – if you develop technology and there should be a loss of life during a terrorist event. Now, it's a very small window but it is something that we should keep our eye on.

Now, the other thing that I think grows out of this and I think maybe was alluded to by the other panelists is shareholder litigation and plaintiff's lawyers. And if you do have standards being set and industry standards developed within the industry – and I strongly endorse what I hear Jamie saying, which is let the industry develop these standards and set some thresholds that are important.

And also I note that the American National Standards Institute's recommended guidance for safety and security in facilities is something that Tom Ridge endorsed in a surprising way. I think no one expected Secretary Ridge to endorse this in testimony.

MS. GORELICK: And you were very helpful in that, Joe. Thank you.
(Laughter.)

MR. WHITLEY: Before your commission – the 9/11 Commission at the New School in New York and I was just delighted that Tom did that. And I think that that's a precursor of other things that Jamie touches on that will be in our future.

There's more I could say and the last thing I will say, though, is the Critical Infrastructure Information Act is also a beginning opportunity for there to be a dialogue, and Jamie says so on this as well and so did some of the other panelists. How do you have information that can be shared with the government in a way that's really meaningful and protected against – again every person that had L as the first letter in their last name when I was going through my confirmation who were all good Democrats on the Homeland Security Committee on the Senate side asked me questions about FOIA and the Critical Infrastructure Information Act and how I felt about it. And I said, judiciously I hope, well, I don't really know that much about it but I look forward to learning about it and talking to this committee again when I have the chance to look at it.

I now believe that – since I'm now free of those bonds – surly bonds that have you wrapped up when you're in office, I do believe that there needs to be some degree of protection. There has to be this balance between the public's right to know and shareholders' ability to invest in the right company, but at the same time I don't think companies are going to step up to the point that they feel like al Qaeda has got a roadmap to their facility. And I think none of us are saying that would happen in these disclosures, but a fear is even government can't be trusted, obviously – not surprising. Government can't be trusted with this information.

MR. CROWLEY: We'll now open up to questions from the audience. If there are, for example, any media representatives that want to ask the first question, by tradition you kind of do that but whoever wants a question please raise your hand and wait for the microphone and identify yourself as you ask your question.

MR. WHITLEY: The risk you run is us to keep talking.

MR. CROWLEY: That's okay.

Q: (Off mike) from Hampshire Research Institute. I notice in the handout you have a second pamphlet on risk management plans. Okay, in your pamphlet package there's a second pamphlet on risk management plans. Can any of you address that subject? I don't know whether you took that into account in looking at market-based mechanisms, but at its heart it is utilizing information at a broader concept of the market. It is not only industry, but the public, academia, the (unintelligible) can look at industry attempts. And also it tries to drive additional planning at the industry level as opposed to looking at financial incentives alone. Can any of you speak to that?

MR. HOUSMAN: The report that's in the folder is on a chemical security survey that we did earlier this year to assess whether chemical facilities – to what extent they are utilizing, to use an environmental term, inherently safer technology but what it really is, is moving from something that is acutely hazardous to a process or a technology or an operating methodology that is more secure, and our findings were mixed.

On the one hand, it showed that there were 284 chemical facilities over the past six years, many of them were drinking water and waste water treatment facilities, that had moved from chlorine gas, which is one of the more serious and potentially dangerous chemicals that a terrorist could exploit, for example, to either liquid bleach or ultra violet radiation, which in the case of liquid bleach may still have environmental concerns but do not really have terrorist concerns. That was the good news that showed that companies on their own through a combination of approaches were moving in the right direction.

The bad news in the survey was that of those 284 facilities, only 10 percent of them were really the high-risk facilities – those that threatened at least 100,000 people in the area surrounding the plant. And so if you put that across a linear baseline, you will solve this problem in 45 years, and from a security standpoint that's probably not good enough. And that's actually part of what is being debated on Capitol Hill literally as we speak. In the mark-up within the Homeland Security Committee is whether you want to put in to legislation some sort of regulatory scheme that gives DHS the authority to work with the chemical industry more aggressively and set standards and then oversee the industry as it meets those standards. And then also whether you want to put in legislation – whether inherently safer technology should be among those tools used. And then finally whether in promulgating a federal standard what that means in terms of state standards; whether they can meet the federal standards, in some cases states like New Jersey currently have a higher standard.

But this issue is the example of where the industry has not necessarily coalesced behind a single group or a single segment of their industry. And actually the ACC, for example, is supporting regulation primarily because they believe they are at a competitive disadvantage because many in the industry – perhaps smaller players – are not meeting the same security standard.

Q: Thank you. I'm Rob McKiernan (ph). I'm the lawyer with the AFL-CIO Office of Investment. We have had some concerns regarding this issue of government and particularly I want to commend you on this very excellent report. The role of homeland security in essentially fostering this debate – we've had the concern with voluntary organizations like the Retail Industry Leaders Association that Wal-Mart is of course a dominant member of, they have actively resisted port security improvements. Wal-Mart's supply chain, as we all know, is 60 to as high as 75 percent dependent upon foreign imports and they have actively lobbied in Congress, even over the objections of Duncan Hunter, to oppose improvements, even taxes or voluntary measures to improve port security.

We've written to the chairman of the audit committee at Wal-Mart because our friends hold sizable investments in Wal-Mart and asked the company to disclose these issues and have got no response. Wal-Mart obviously operates on the lowest cost principles consistently. I think that it underscores Jamie's point that we really need government to take a proactive role here through DHS as well as SEC to begin to push companies to take this issue.

This is fundamentally a national security and an investor security issue. If it isn't done, though, we can't rely essentially on voluntary organizations of industry to do itself. The Wal-Mart example I think is a – and the retail industry leaders' one – is a perfect case in point. We really need DHS or the Department of Transportation to say, "Look, we're going to convene this group of industry and begin to bring this debate forward." Otherwise, investors are left in the dark, as we are. And I can certainly share this correspondence with anyone on the panel. It's quite a big concern.

MR. CROWLEY: Picking up on the point, is government's role to promote a process as opposed to promoting a standard?

MS. : What do you mean?

MR. CROWLEY: I mean a process in the sense that you're promoting a system of collaboration through which you would expect security to improve, as opposed to a formal regulatory scheme where you mandate a certain level.

MS. GORELICK: If you take the NSTAC example, you get both common standards and you get a process for sharing information on threats, for sharing processes for responding to an attack. This question is different than that because what we have been talking about are the standards that a company would follow in its own actions and its own work, and not the positions that it would take with regard to, say, the cost of a supplier, which is essentially what I gather the Wal-Mart position would be with regard to the ports. So I don't know that anything at least that we've been talking about addresses that.

MR. HOUSMAN: I think it does if I can for on quick second. I think this is P. J.'s bet-the-ranch example. A company's position vis-à-vis pending legislation that might have a material impact on its operation should be disclosed. I think in this instance it's actually acting outside its own best interest and the shareholders should know it because let's take the example of Vayl Oxford, the head of DNDO the Domestic Nuclear Detection Office within the Department of Homeland Security has said that there's an absolute certainty, he believes, that in his life time a nuclear device will be smuggled in to the United States via a cargo container and used against one of its cities. That's a DHS official who is in his area of responsibility saying that.

If that occurs, numerous experts have said that what will happen is every single port in the United States will close for a matter of days or weeks. The direct impact on Wal-Mart will be Wal-Mart will be shuttered within a matter of days. It's a just-in-time

operation. If it doesn't have access to its supply chain, there is no more Wal-Mart. That is a risk that the shareholder needs to know exists. I would argue, and others might differ on it, but if I were advising the company I would say that that is a material risk.

MR. WHITLEY: Let me just free associate a bit, but the Customs Trade Partnership Against Terrorism, or CTPAT, which is a process whereby you get better treatment if you do certain things with CB – Customs and Border Protection, otherwise known as Customs I suppose, so you get a break there. That's a voluntary system right now. It may be moving toward a statutory regime.

The other is the Container Security Initiative, which is the overall initiative which means pushing our borders further out and we have people in ports around the world, there are customs officials that are helping identify higher risk containers. All that being said, how do you drive some change in this area so you have a higher degree of confidence that the supply chain will be protected? This may be beyond the reach of God almost. So I would say that the challenge, though, is – and I think with government always – is I think Jefferson said something to the effect of you can trust people with their government so long as they are well informed. And I think the challenge is on this issue, the challenge and the risk are the same maybe, is that Congress – in maybe not such a well informed status post-event might further kill the goose that laid the golden egg.

And I think the challenge is finding the right balance between flooding Wal-Mart stores with everything they possibly can get in there so you're – the people that are involved in the fund will get a great return on their investment and at the same time might lose it. I don't really have an answer, but I think it lies in an aggressive involvement by people involved in the supply-chain industries coming to the table affirmatively, like ACC is seeing, and aggressively embracing some standards that they feel they can fit. In other words, when you go buy a pair of shoes if you have a size 13 foot like I do, you don't run in and buy a pair of size nines. So I think this has to fit each industry the way each industry is set up.

MR. HOUSMAN: What is the lesson from, say, Sarbanes-Oxley? I mean, one would think that as a properly run business you would balance the books and you would do the right thing and you would know what's happening inside your company. But now we know that that didn't happen so now you've got this remedy that if nothing else it requires the CEO at the end of the day to sign the bottom line saying I know what's in this report and to borrow the phrase from (unintelligible) politics, I endorse this message.

To part of the thrust of Rob's report, how do you bring that level of corporate scrutiny on security in to the boardroom? CTPAT is a great example wherein it's voluntary right now and you kind of do a one-off application, it's reviewed by DHS, and then everyone says everything is in place, but there's no real follow-up. I think there's a great analogy here where if you do have critical operations, you should do annual third-party security audits and be required in some fashion just to say we're paying attention to security, we believe it's adequate to our operations. It's not necessarily saying how

you're going to secure your supply chain if it's Wal-Mart, but that you affirmatively state that in your view you have done the best job you can.

MS. RUTKOWSKI: I think that's a really good question. It sort of takes you back to the debate about accounting and about a lot of SEC issues in general. Do you want a rules-based or check-the-box (type of?) audit or you want more of a principles-based approach with some thought about this and this and that, which takes me back to Jamie's suggestion: industry groups with some guidance or protection from the government would seem to be a good balance because it would be more flexible. You certainly don't want the top-down, heavy-handed legislation dictating because they're always going to get it wrong. And the agency coming from the ground up is never going to quite get it right. So you need the industry in there, but the question is do you need legislation? Could you do this in industry groups currently? And if you do need legislation what would it look like?

MS. GORELICK: Let me just say that the analogy to Sarbanes-Oxley raises precisely the question that I've been putting on the table, which is you certify to what standard? I mean, Sarbanes-Oxley launched this 404 process by which there had to be a certification that your books and records were appropriate and that was launched before there were clear standards by which the auditing firms were supposed to give their advice. And it led to a tremendous amount of confusion, huge audit fees, a lot of – I think everyone would say much of the effort was not productive, and so if you launch something like that without knowing what is good, what is something you should aspire to, then what are you certifying?

You're launching a bunch of consultants to say you're secure. It's a good investment in a consulting firm, but not necessarily going to get you some place unless you're thoughtful about what security means in the context of this company operating in this place in the world performing these functions. And that is a down-and-dirty, flexible set of standards that has to emerge from companies themselves with in my view assistance from the government. I'm totally with Joanne here: if you have this prescriptively, you are creating a lot of work for very little productivity.

MR. CROWLEY: I want to ask Joanne a question. I agree with that, I would associate myself with all those remarks. My one question on SOX, though, is – and I think it's a question of did they put the cart before the horse quite frankly. Granted, fees have been high; granted, missteps – my understanding is that the industry in response to SOX has actually come up with standards and now there's a growing understanding of what it is we mean by appropriate.

MS. RUTKOWSKI: And also, I mean, the goals and the policy purposes of Sarbanes-Oxley I don't think anyone argues with. But just the question of how do you get to that end point. You know, Sarbanes-Oxley was 2002; this is four years later.

MR. CROWLEY: Last question I suppose would be and part of this with whatever final comments you want to make. Currently right now there is legislation on

the Hill in both houses of Congress. I don't know that it sets a prescription for what the chemical industry would need to do. What it does do is give DHS a right to have a meaningful conversation with the industry so that standards can evolve. Is that the right answer or do we think that we don't necessarily need formal legislation that allows DHS to knock on the front door, that this is something that should evolve more naturally. What's the lesson from what's happening right now and then any final comments each of you might have?

MR. WHITLEY: Just a word or two on that since I'm the only former DHS person up here. I do think that the Maritime Transportation Security Act – MTSA – is a good template to think about, and I think Congress is struggling with whether or not to use that with the chemical plant security legislation. I think it more than anything else gives industry some broad parameters in which to operate.

And I believe that the opportunity to observe industry function within something that gives them a great deal of flexibility and freedom is a better model where each port facility or vessel has to come up with its own compliance plan to deal with safety or security issues, and this is overseen by the Coast Guard. In a way, it also becomes a huge resource issue, too: if we put in place too many regulatory or statutory frameworks, we end up spending all of our time dealing with those issues to the points that have been made by the people up here.

I always felt like this would be my dream and I'll end on one I-have-a-dream moment. (Laughter.)

MS. GORELICK: Go back to sleep again.

MR. WHITLEY: Yes, the dream speak. And so if I wake up this morning thinking about this, what was I thinking? And I wrote it down and it was what we want to see is this sort of – instilled in the sort of the breeding of corporate America as though when we step into an automobile and put on a safety belt today. We do that automatically. And I think industry, in order to get to that place, and I think it will take a degree of encouragement to industry to do that, but I think it needs to be done in a way that doesn't so constrain us that we don't have the economic engine working the way it should work.

MR. CROWLEY: Final comments?

MS. GORELICK: I have nothing to add.

MR. CROWLEY: Final questions? Good.

Q: (Off mike.) I'm sorry. Edward Roeder, Sunshine Press. Do any of you know of any instances where any companies have faced successful shareholders lawsuits for their failure to comply with the SEC requirements you set forth in disclosing their security vulnerabilities and how that could affect their bottom line?

MS. RUTKOWSKI: I'm not aware of any and I think one point which Rob made in the report is most companies don't consider these material issues, so there wouldn't be a disclosure obligation in the first place.

MR. HOUSMAN: You'd have to premise it on a big event. There would have to be something that happened that really impacted the shareholders so that they could go in and say, look – the only instance that I know where it could have been would have been something like Three Mile Island or 9/11, and nobody filed a shareholder suit on 9/11 and my belief is that the statute of limitations is run. But it does surprise me no one has actually.

Q: If the SEC won't enforce the law and nobody sues and the marketplace isn't enforcing the law, why should anyone care? It seems that this is a matter of national security where the marketplace doesn't matter or doesn't care, the courthouse doesn't care, and if the government doesn't enforce it, how is it going to happen?

MS. RUTKOWSKI: I think all three constituencies care very much. It may just be a case that you haven't had another 9/11. This is the post Katrina syndrome, we're just waiting for the next hurricane.

MR. : Well, I must say I don't think anybody – I mean, not to pat ourselves on the back, but to pat ourselves on the back, nobody has really looked at this yet. This is the first time anybody has said – to the best of my knowledge, this is the first time anybody has said companies would have a disclosure requirement for material security information. I think most of the corporate sector hasn't focused on it.

MS. GORELICK: I mean, you have to even think about who you could have sued. You could have sued the airline in which you'd invested because they didn't disclose that if there was a catastrophic event involving a terrorist using airplanes that airplanes would sit on the ground and the stock of the airline would go down. I mean, it would have really been a reach in that circumstance. So I think what Joanne is saying is, well, now that we're focusing on this, as Rob says, you have this report. It may be that raising the issue of whether this kind of disclosure is necessary to meet the materiality requirements will increase with people thinking about it and disclosing, but I cannot imagine a court saying to American Airlines, "You should have put in your disclosure this risk," when you have the entire government saying how totally unanticipated and unanticipatable it was.

Q: For example, all the utilities have their tank farms and their nuclear reactors along major waterworks. They are extremely vulnerable to various kinds of attacks.

MR. CROWLEY: I think the final answer is, looking backwards Jamie is of course correct. The issue is the next one is going to be less of a surprise and so I think a lot of these forces that come together, many of them destructive from a broad societal standpoint – I mean, the thing about the victims compensation procedure was it worked

as it was designed: we focused on rebuilding, we didn't focus on recrimination. The next event, God willing we don't have one, but if we do I think you'll potentially see a different dynamic unless you have a better and stronger system in place. I think that is the underlying message behind the report.

We thank you very much for attending and we thank our panelists and congratulations to the authors and we're adjourned.

(Applause.)

(END)