FINAL TRANSCRIPT

Thomson StreetEvents℠

**ACC - The Legal Aspects of Homeland Security

Event Date/Time: Dec. 08. 2004 / 1:00PM ET

CORPORATE PARTICIPANTS

Rob Levin
Moderator

David Mendelsohn
Piper Rudnick - Partner in Homeland Security and Insurance Practice Groups

Jay Westermeier
Piper Rudnick - Partner in Business and Technology Practice Group

Kevin Mullen
Piper Rudnick - Partner in Homeland Security Practice Group

Jim Halpert
Piper Rudnick - Partner in e-Commerce and Privacy Practice Group

Deborah Rosenbloom
The Cohen Group - Vice President

PRESENTATION

Rob Levin - *Moderator*

Good afternoon and welcome to the Association of Corporate Counsel Webcast on The Legal Aspects of Homeland Security. I'm Rob Levin (ph) and I'll serve as moderator for this Web cast.

A few years ago, Piper Rudnick authored the first Association of Corporate Counsel Homeland Security info pack. This year, Piper Rudnick was asked to update the info pack. However, because of the rapid developments in this area over the past two years, a complete rewrite was in order. The new info pack was introduced and distributed at the ACC Annual Meeting in Chicago in October of 2004, and now serves as a reference document for this ACC Web cast.

Hopefully you have all had a chance to review the info pack. If you haven't, the presentation today will provide you with a good overview of some of the legal aspects of homeland security. Because it would take much longer than an hour and a half to discuss the entire contents of the info pack, panelists of this Web cast, including Piper Rudnick attorneys and representatives from the Cohen Group will be discussing a handful of topics covered in the October 2004 Homeland Security info pack. These topics include corporate viability and business continuity, cybersecurity, the SAFETY Act, the Department of Homeland Security and information sharing and the Freedom of Information Act.

For those of you who don't regularly practice in this area, I think you'll be impressed by the diversity and the importance of the issues that fall under the term Homeland Security and by the insights that our panelists today will offer on both the legal and business issues raised.

A brief Q&A session will follow this presentation. Our first speaker is David Mendelsohn. Mr. Mendelsohn is a partner in the Homeland Security and Insurance Practice Groups with Piper Rudnick. He concentrates his practice in the areas of general, corporate, technology and insurance matters. Mr. Mendelsohn has extensive experience representing clients regarding the development and implementation of enterprise wide initiatives designed to bring organizations into compliance with various legal and business requirements, as well as structuring and preparing compliance training and ethics programs.

David will speak on corporate liability and business continuity matters as they relate to fiduciary obligations imposed on directors, officers and management in a post-9/11 world. David?

David Mendelsohn - *Piper Rudnick - Partner in Homeland Security and Insurance Practice Groups*

Thank you, Rob. This is David Mendelsohn. I'm a partner with the law firm of Piper Rudnick, which I'm happy to say will be DLA Piper Rudnick Gray Cary on January 1st, so I'm glad we're doing this in December because I can take up less time saying our name.

What I'm going to try and do in the next 10 to 15 minutes is provide something of a backdrop for the remainder of the presentations today and try and convey why it is important for businesses to address homeland security issues from a management and liability management perspective.

If we take a look at the PowerPoint presentation that hopefully you have in front of you, slide number 4, first reference is to the National Strategy for Homeland Security, which is the publication that came out in the summer of 2002 from the Office of Homeland Security. And what that did it, really, was present for the first time an official statement from a government-related body that indicated it was paramount for businesses to assess risks associated with security issues, invest to protect key assets of their businesses, and treat homeland security essentially as a matter of corporate governance and good corporate citizenship, and they viewed this as essential for safeguarding the interests of the shareholders and employees.

It was followed by numerous other publications along those lines, and ultimately the Homeland Security Act was passed that essentially evidenced the government's expectation that the private sector would work with the Undersecretary of Information Analysis and Infrastructure Protection to provide information on infrastructure and vulnerabilities of the infrastructure, to work with the government to identify priorities to protect critical infrastructure, and also to provide and/or receive information and advice on protective actions and countermeasures that could be taken with respect to the infrastructure.

Why was all of that so important? Well, if you take a look at some of the statistics on page five of the PowerPoint, you will see 80% of terrorist attacks in the last 30 years have targeted businesses. That's a statistic contained in the State Department's Annual Report on Global Terrorism in 2001.

The often cited percentage of 85% of critical infrastructure that is owned and operated by private enterprise is somewhat surprising when you first hear it, but then sometimes it's as high as 90%. But what that really tells us is that critical infrastructure of this country is in the hands of private enterprise, in the hands of business. It is not under the control of government, at least not direct control, which is why in the May 2004 report from the General Accounting office, there's a statement indicating that it is the responsibility of owners of critical infrastructure in this country to protect that infrastructure.

So clearly, terrorism activity historically has targeted business interests. Most of the critical infrastructure of this country is in the hands of private enterprise. It is not surprising therefore that the Business Roundtable in the US, which is comprised of the CEOs of rather substantial companies and which attempts to devise a set of best practices, which are designed to guide corporate governance, focused on the security issue in the last year, year and a half, and essentially created an objective that businesses create business resiliency. And they want -- the best practices that they outline require companies to engage in risk assessments and management, focus on business continuity issues, address physical and cyber security issues and cyber security was identified as a corporate governance issue in May of 2004 by the Business Roundtable, and also to focus on emergency communications.

So you would start to work your way through the evolution of all of this. The terrorists target business, businesses own the critical infrastructure, corporate executives identify best practices that are designed to effectively create this business resiliency.

How has this all manifested itself or what has it developed into from a corporate practice standpoint? Well, spending on security has definitely increased, perhaps by material amounts, so there is definitely a shift towards addressing some of these issues, although as I'll mention in a few minutes, certainly there is indication, at least with respect to business continuity planning, that still companies are not as invested with that aspect of their preparations as perhaps they might be, but in any event, I think what September 11 has managed to do for us all is provide us with a sense that these are new risks we are contending with, which require new thinking and approaches.

Now, the next slide, slide number 6, is where a lot of the standards, really, references - there are a couple of areas where standards have begun to evolve. We start out with officers and directors of companies and the fiduciaries of their companies, and they owe fiduciary responsibilities to act in good faith and in the best interests of their corporation, to minimize or eliminate liability for the organizations and protect the goodwill and preserve the assets of their companies. Undisputed, they have a duty of care in that regard.

The business judgment rule provides protection to management. Business judgment rule, for the most part, says that if management makes a well informed decision in good faith, they're protected, even if it's a bad decision, even if it's a wrong decision, even if it's an erroneous decision. But the interesting decision out of the Caremark case in 1996 really expanded the scope of the responsibility of directors and officers to devise information systems within a company that allows timely and relevant information to be brought before management before they make informed decisions in good faith in the best interests of their company.

So it is the responsibility of management to essentially oversee the creation of systems within the business, within the company, that allows them to receive up to date and relevant information that allows them to then make management decisions that need to be made. In the context of homeland security what that really means is that they have to have people working throughout the organizations that make assessments of risk, identify concerns or issues and feed that information up at the Board level or at the executive level so that the right decisions can be made.

Now, interestingly in the context of 9/11 we've seen some litigation that starts to put a little bit of context in this area or develops a little bit of context for this area. The legislation that followed September 11, the Air Transportation Safety and Systems Stabilization Act of 2001 essentially says that victims of the events of 9/11 could either obtained compensation through the government's Victims Compensation Fund or they could otherwise use the courts to obtain their own relief.

Most victims decided to side with the fund and have sought recovery through the fund, however a good number of victims or family members of victims decided that they would pursue litigation, and by virtue of that statute, all of the claims were consolidated and are being decided in the federal court for the 7th District of New York.

Now the defendants at issue in that litigation are the airlines, the airport security companies, operators at the airports, owners and operators of the World Trade Center and the Port Authority of New York and New Jersey, and also Boeing, which manufactured two of the planes in question. And in a decision that now is a few months old, there was a discussion about whether and to what extent these defendants owe duties of care to the victims and family members of the victims.

And what is quite revealing in the decision was that there was considerable focus on the duty of care owed in this instance perhaps by an airline for example to individuals who were on the ground who may have been hurt as a result of the planes crashing as well as the security companies knowing full well that if they didn't do their jobs adequately, that good result in a lack of security, which could create some kind of risk and some kind of incident. Boeing's failure to properly design -- allegedly to properly design the aircraft to make them safe, failure of owners of buildings to develop adequate evacuation or emergency management plans, those kinds of obligations were being raised and the defendants were saying this is too extensive, we don't owe these kinds of obligations.

So what the court went through was an analysis to identify 1) whether there was a duty of care; 2) what was the scope of the duty; and then 3) what was the standard that would give rise to a breach. And focusing on a number of different factors -- there were five factors -- the court essentially concluded that there were duties of care that were owed based on reasonable expectations of third parties and what these companies were doing. The fact that the class of claimants that may raise a claim for breach of the duty was a determinable class, so that it wasn't a limitless class, that the liability of the defendants could be ascertained and that it wasn't an unlimited form of liability that perhaps would run against public policy. They focused somewhat on the relationship between the plaintiffs and the defendants, and ultimately concluded that this wasn't going to create new channels of liability.

So they essentially said that a duty of care existed and because the plaintiffs ostensibly were within the zone of foreseeable harm, that they fell within the scope of the duty and then the standard that was devised essentially was one of reasonableness, saying that if there was a breach of duty, it's because the defendants failed to act reasonably in the circumstances.

So then that raises the question what is reasonable in the circumstances. Well, it's easy to say that before 9/11 there really was little precedent to suggest that terrorism activity was foreseeable. Now I think it's much easier to take the position that terrorism activity is foreseeable and that most people's mindset is it's not a question of if, it's just a question of when and how.

So if you take a look at the standards that appear to be developing in the 9/11 litigation, and you combine those standards with the standards created by Caremark and the fiduciary standards that management have, and combine it also with the standards now evolving under Sarbanes-Oxley to make sure under Section 404 that there are procedures in place to make sure that information flows through the organization sufficiently to allow executives to sign off on financial statements and other filings made with the SEC, it's very easy to make an argument that management has significant responsibility to think about homeland security issues or any other kind of security issues, both physical and cyber security, and address them.

So that's really the background that I was asked to develop for the rest of the presentation. What I was also asked to address briefly was the concept of business continuity, particularly in light of some recent developments in that area. BCPs on slide 7, business continuity plans, are something about which we've probably all heard a great deal.

I sit in Chicago and just two nights ago, the LaSalle Bank Building right in the heart of downtown had a pretty bad fire. But if you were to speak to any representative of LaSalle or call somebody that you know at LaSalle the next day, it was very apparent that they had very sophisticated business continuity plans in place and that they didn't really miss a heartbeat in terms of their operations.

I can't think of a better example of seeing a business continuity plan under operation, although perhaps the blackout that we all witnessed on the East Coast just a few months ago is also a very good example of how the financial services industry really was primed for an event like it and could respond well. Interestingly, when the blackout occurred, the Dow Jones index rose a handful of points, which just shows that marketing continued and that trading wasn't severely impacted. That's probably as good an indication as any that business continuity plans were effective.

Good business continuity plans really seek to mitigate the consequences and the duration of potential disruptions. There's lots of literature about process that one engages in to develop and devise business continuity plans, but recently, just a few months ago with the SEC's approval of the New York Stock Exchange and the NASD developed their own rules essentially, they authored their own rules that were approved by the SEC about what their member firms should develop and provide for in the business continuity space.

Now these roles are interesting in the sense that I think what they do is create a standard again, which other companies can strive to achieve and they really identified, and I laid them out on page 8, 10 fundamental elements of business continuity that the members of these two organizations must seek to include within their business continuity plans.

What the rules also recognize is that these plans need a good deal of flexibility, recognizing that members are not all in the same situation, they recognize that some of the 10 requirements may not apply, so they allow for flexibility and they allow for companies to devise plans that don't include all of the 10 elements, but they have to explain why they don't if they don't. They also require disclosure of the business continuity plans, and this is a big factor I think that in these provisions.

There are generally two reasons for requiring disclosure of the principal terms of the business continuity plans to the consumers. One, to give the consumers confidence that in the event of some security breach or disaster, that reasonable preparations have been made and will be executed to ensure reasonable fund availability and security. But the second is perhaps more interesting and more defining, and that is that they think disclosure creates industry pressure and provides businesses with the opportunity to create a competitive edge.

So what we're seeing with business continuity over the last several years is the development of an approach where, first of all, it was considered to be mostly an IT issued to one that now is considered more of a business issue and now one that is considered perhaps something that needs to be disclosed and a way of getting a competitive advantage.

When you take a look at the minimum requirements on page 8 it's easy to see how some of those may relate to your business, whether you are in the financial services industry or otherwise, but it really focuses on some of the things that I mentioned were part of achieving business resiliency and part of the best practices devised by the Business Roundtable at the outset of my comments. There's focus on communication, there's focus on risk assessments, there's focus on employees, and it really is not difficult to see some element of consistency in what it is that businesses address.

A recent European survey just indicated that there are still a very substantial number of businesses where they do not have executive involvement in the development of BCPs. Over half of companies, according to the survey, do not have the involvement of executives in BCPs. That troubles me as a lawyer, when advising management, because I don't think it is necessarily an easy thing to assert that you've somehow satisfied fiduciary responsibilities in light of Caremark and it's not easy to assert that you're in a position to defend any allegations that may flow in litigation like the September 11 litigation if management and the Board are not involved in these kinds of issues and in the approval of the approach that's taken to develop these plans internally.

Last slide for my comments, slide number 9, and just quickly focusing on the blackout that occurred in 2003, it really provided a sense of how business continuity planning can really benefit business in a difficult time. It was business as usual for the financial services industry. Trading continued on the floors of the exchanges, and I think there was a good deal of advantage that was gained by the sophisticated proponents of these plans because they try to account for what are called cascading failures, where you think through what might happen in the event of a disaster and you allow for the falling of the dominoes that can flow from the loss of power on the Eastern Seaboard to some other catastrophic event, whether it's a hurricane or a September 11-like incident.

Clearly, lessons learned from the blackout were, and I think this is clear, that you focus not just on IT issues and backing up data and preserving records, but you focus on non-IT issues and you view your business globally in trying to assess what the impact might be in the event of a catastrophe or some disruptive event. You can't just develop a plan and then put it away on the shelf and hope you never have to use it.

The LaSalle Bank Building engaged in a fire drill and some training on their business continuity planning just weeks before the fire of two nights ago and no lives were lost and their business continued to function very smoothly, and I think that's indicative also of how regular testing and updating works to your benefit. And then come back to my other point, which is my last point today, and that is use BCPs to create a competitive edge. There's an opportunity to distinguish your business from the business of your competitors, and that can only inure to your benefit and the benefit of your Company.

I think that concludes my remarks, thank you.

Rob Levin - *Moderator*

Thank you, David. Please note that we'll take your questions during the Q&A session which will be at the end of the panel discussion. Please e-mail your questions during the Web cast to Homeland@PiperRudnick.com.

Our next speaker is Jay Westermeier. Mr. Westermeier is a partner in the Business and Technology Practice Group at Piper Rudnick. Mr. Westermeier is the only lawyer ever to receive the Distinguished Information Sciences Award, the highest award presented annually by the Association of Information Technology Professionals. He is past President of the Computer Law Association, which is the world's largest association of its kind, members in 60 countries. He also served as Chairman of the ABA Committee on Professionalism of Computer Specialists under the Science and Technology section. Jay will discuss the legal ramifications of cyber security.

Jay Westermeier - *Piper Rudnick - Partner in Business and Technology Practice Group*

Thank you very much, Rob. Cyber security, make no mistake about it, has really become a boardroom issue. In fact many of us believe that in the coming years cyber security and security will be practice areas in and of themselves, substantive areas that we will be focusing on in the years ahead.

So cyber security has become very very important. Topics like fishings, spyware, and identity theft have become major problems. The risk of computer hackers, computer viruses, and worms, denial of service attacks, theft, terrorist attacks, sabotage, surveillance and intrusion by competitors and malicious acts by disgruntled employees, and many other vulnerabilities are increasing at an alarming exponential rate.

Managing the risk from these unprecedented threats to the enterprise has become a vital risk management concern of the Company's Board of Directors and top management. The result today is that effective cyber security programs have become a legal necessity. Prudent risk management and due care with respect to cyber security programs are indeed necessary to avoid potential legal liability.

When we talk about cyber security we're talking about a risk management process, a process to protect the confidentiality, integrity, and availability of information systems and information content. In the short time that I'm going to be talking with you, I want to discuss the five FTC, that's the Federal Trade Commission, cases that deal with complaints that were filed against companies for inadequate information security, and I want to talk about the legal significance of these five consent orders and what they mean to companies.

If you look at my first slide, which is slide 11, we talk about the importance of the FTC consent orders. In these five consent orders, and they all focus on information security, the respondent companies were each required to establish and maintain a comprehensive information security program in writing that was reasonably designed to protect the security and confidentiality and integrity of personal information collected from or about consumers.

The importance of these cases cannot be underestimated. The Tower Records case, Guess case, Microsoft, Eli Lilly & Company and more recently, in November of this year, the Petco animal suppliers case, all of which deal with flaws in Web sites and information securities.

The Eli Lilly case was a situation where an employee had sent out notices to the Prozac users for Eli Lilly and had sent it to all of the Prozac users and so that every Prozac user knew who every other Prozac user was, and the FTC found this practice to be actionable under Section 5 of the FTC Act. Very very important aspect here because the case emphasized the fact that in every information system, training is an integral portion and a very important portion of computer security. In that case, it was a brand-new employee who had been tasked with this obligation to notify the consumers and he had no training whatsoever, and in fact, was ill-prepared for his responsibilities and obligations.

Let's talk about these consent orders. If you look at my next slide on 12, we talk about the fact that the consent orders each required the respondent to maintain an information security program containing administrative, technical, and physical safeguards appropriate to the company's size and complexity, and the nature and scope of its activities. The information security program that was necessitated by the risk and had to be commensurate with the level of risk that the company was involved in. After all, we emphasize the fact that cyber security is a risk management process.

The four fundamental ingredients are shown on slide 13. These were the ingredients, the components, that the FTC indicated were necessary for a comprehensive information security program. Step one, accountability. Companies should designate an employee or employees to coordinate and be accountable for the information security program. Step two, risk assessment. Companies should identify material internal and external risk to the security, confidentiality and integrity of information that

could result in the unauthorized disclosure, misuse, destruction, or other compromise of such information and assess the sufficiency of any safeguards in place to control these risks.

The FTC goes on to say at a minimum, this risk assessment will include consideration of the risks in each area of relevant operation, including one, employee training and management; two, information systems, including network and software design, information processing, storage, transmission and disposal; and three, prevention, detection, and response to attacks, intrusions, or other system failures.

The third element is safeguards. Here the FTC requires that companies design and implement reasonable safeguards to control the risk identified in the second step through the risk assessment and regularly test or monitor the effectiveness of the safeguard's key controls, systems, and procedures. Fourth, the FTC requires that companies maintain their information security plan and evaluate and adjust their information security program in light of the results of regular testing and monitoring, as well as any material changes to the operations or business arrangements or any other circumstances the company knows or has reason to know may have a material impact on its information security.

These FTC cases and the elements making up the Comprehensive Information Security Program are not well known and had not been given wide level of mention in the literature, and I believe that it's a legal standard now that companies need to be able to assure themselves that they are meeting these minimum requirements for a Comprehensive Information Security Program to avoid potential legal liability.

The last couple of FTC cases have added to these four elements a requirement for an independent assessment, and the independent assessment in the Tower case was required to be conducted within six months of the order, as well as having biennially thereafter every two years for a 10-year period.

And the independent consultant must be a certified information security specialist or one of the other categories recognized by the FTC as having the necessary level of credentials to provide an independent assessment of the security program. And when we see that the FTC has challenged security flaws, make no mistake about it, we're seeing evidence of the minimum security requirements and minimum security standards that could give rise to legal liability in the future.

These cases establish the minimum liability standards that could in fact have collateral significance in other proceedings and other matters and other legal causes of action. And I think there are a lot of things that the legal department and companies can do to improve the legal aspects of Comprehensive Information Security Programs to include developing legal battle plans to be part and parcel of response for cyber incidents. I'm going to end at this point in time. Thank you Robert.

Rob Levin - *Moderator*

Thanks, Jay. Again, if you have any questions we'll take them at the end of the presentation during the Q&A session. The e-mail address is Homeland@PiperRudnick.com.

Next up is Kevin Mullens. Kevin will address us on the SAFETY Act, which is a piece of legislation which provides broad liability protection for contractors who are selling anti-terrorism technologies to the government and to private customers. Mr. Mullen is a partner in the Homeland Security Practice Group at Piper Rudnick. He has experience counseling clients involved in homeland security contracting, including vaccine development and production, biological, chemical, and radiological detection products, and security services. He represents clients seeking liability protection under the SAFETY Act, and under government indemnification under other federal laws and provides related counseling concerning product liability insurance coverage. Kevin?

Kevin Mullen - *Piper Rudnick - Partner in Homeland Security Practice Group*

Thank you, Rob, and good afternoon. You'll see in your materials, starting on page 14, I'm going to talk about the SAFETY Act and liability protection for homeland security products and services. On page 15 you will see that that acronym, the SAFETY Act, stands for Support Antiterrorism by Fostering Effective Technologies Act of 2002. It was part of the Homeland Security Act passed by Congress in November 2002 that David Mendelsohn mentioned in the opening remarks of this program.

And in particular, the SAFETY Act provides new statutory liability protection for qualified anti-terrorism technologies in the event of a terrorist attack. Now, it's important to note that the liability protection, as powerful as it is, and I'll describe its scope in a moment, is limited to the situation where a terrorist attack has occurred. It will not provide your products and services with any kind of liability protection outside of those circumstances.

The scope of the SAFETY Act is significant, and as a first example of that, is that it applies to the sale of your products and services, if they qualify, both in federal, state and local government contracts, but also in all of your commercial sales. So it's very broad sweeping and many times people come to the initial and wrongful conclusion that it is limited to government contracts. That's not true, it applies to commercial contracts as well.

The SAFETY Act was the Bush administration's attempt in the Homeland Security Act to address the problem of excess liability exposure that companies providing homeland security products and services would face, and would make them reluctant, even the most patriotic company, to provide homeland security products and services and expose their company to overwhelming and devastating liability.

As I said, the Act was passed in November 2002. The Department of Homeland Security, which administers the SAFETY Act, passed interim rules and issued an application kit in October of 2003.

If you'll turn to page 16 of your materials we'll continue and talk a little bit about the scope of the liability protection that this new legislation provides. First of all, in the event of a terrorist attack, if your product or service is implicated as, in the plaintiff's view, as not having done its job in protecting or mitigating or responding to the terrorist attack, that plaintiff can only bring that case in federal district court. So there is exclusive federal jurisdiction over these third-party claims for liability.

Secondly, that plaintiff has a single cause of action against the seller of the product or service. So subcontractors, teammates, the customer, that is the user of the product or service, are all shielded from liability.

The heart of the SAFETY Act protection applies in the event that you obtain, through the application process at the Department of Homeland Security, what are called designations. This is the standard level of coverage under the SAFETY Act that provides additional proof and a limitation on the damages that plaintiffs would be allowed to recover in the event of a cause of action against your company. And the main components of those limitations are first of all total damages that are recoverable by the plaintiff are limited to the amount of the seller's insurance, and the amount of your insurance is ultimately determined by the Department of Homeland Security through the application approval process.

Second, non-economic damages. They require a showing of physical harm by the plaintiff in order to recover. Secondly, their recovery is limited to the seller's percentage of fault. Next, no punitive damages, very good news. Also, no pre-judgment interest. And finally, the damages that the plaintiff is entitled to are reduced by the amount of any other collateral recovery the plaintiff might realize, for example, through their own insurance coverage. So it's very powerful protection of a seller of these homeland security products.

The second and also viewed as a very important part of this potential coverage is what's called certification. You'll see the fourth bullet on page 16 this is addressed. If you are able to qualify for certification through the SAFETY Act approval process, you will be entitled as the seller/defendant, to a rebuttable presumption of what is called the government contractor defense, and the

government contractor defense is a defense that is developed through case law for government contractors that for purposes of this discussion provide a practical shield from liability for the SAFETY Act approved product.

In essence, if a plaintiff were to bring a cause of action against a seller who was certified in terms of their SAFETY Act coverage, they in my view would be successful in having that case dismissed. So certification is a kind of super coverage, if you are able to satisfy the criteria in the Act and in the implementing rules. It's very important coverage.

The next page of your materials, page 17, attempts to answer the question, how should you view this new legislation. If you're the seller of homeland security products and services, what does this mean for you? First of all I would echo some of the things that David Mendelsohn said about corporate governance. We have a new environment now in the homeland security area and I think the SAFETY Act raises an additional area of corporate governance.

We have here a statutory liability protection that's available to you, to an administrative process that at Department of Homeland Security if you, as a public company, and I would view this in an analogous way for private companies that are trying to be prudent, but especially if you're a public company and you don't avail yourself of that statutory liability protection and you're faced with a terrorist attack and then that follows with a large lawsuit against your company, I think in many instances a shareholder would be reasonable in second-guessing your decision to forego that coverage.

Now, it doesn't mean that everybody will be approved for this coverage, but I do think that out of prudent corporate governance it ought to be considered very carefully and if there is a chance of eligibility for the coverage I think a company should be seriously considering applying for it.

Secondly, the application and approval process at the Department of Homeland Security. In essence, what you do, is through a web site you fill out an application form which admittedly is a complicated endeavor and a little bit too time-consuming for most of the industry preferences, you fill that out and you submit it through the Department of Homeland Security's Web site. That initiates a dialogue with the SAFETY Act office within DHS and ultimately, after about 150 days, you can expect to hear one way or another whether you've been approved for coverage.

The SAFETY Act provides one other element for serious consideration. This goes to the marketing and business folks within your organization. I think it provides a significant potential competitive advantage. First of all, if you are approved for designation and if you're approved for certification, that is, the higher level of coverage, you're also placed on what's called the Approved Product List for Homeland Security, you can advertise those facts first of all, there's nothing that prohibits you from doing that, and in that sense I think it's reasonable to view the SAFETY Act's approval as a kind of stamp of technical approval from DHS. It also provides liability coverage to the buyer of the homeland security product that is designated or certified as SAFETY Act covered. So that is a very important additional value that your product or service can provide and distinguish itself for competitive purposes. So I think that wraps up my remarks. I look forward to answering any questions. Thank you.

Rob Levin - *Moderator*

Thanks Kevin. Our next speaker is Jim Halpert. Mr. Halpert is partner in the e-Commerce and Privacy Practice Group at Piper Rudnick. Mr. Halpert counsels technology and content companies on a broad range of legal issues concerning new technologies, including intellectual property protection, content regulation and 1st Amendment law, privacy, government, surveillance, standards, Internet jurisdiction, telecom regulation, online contract formation, Spam and domain name administration. His counseling practice includes advising copyright owners, ISPs and equipment manufacturers regarding anti-piracy infringement and copy protection technology strategies and advising a wide range of companies regarding privacy and computer security issues. Jim will speak on critical infrastructure information as it relates to the homeland security market.

Jim Halpert - *Piper Rudnick - Partner in e-Commerce and Privacy Practice Group*

Thanks very much Rob. This is another part of -- or another set of regulations that developed from the Homeland Security Act of 2002, and its genesis really comes from the same kind of theory that prompted the SAFETY Act that Kevin just explained. Because the private sector is the source of so much of the critical infrastructure and the private sector can bring information to light to government about security problems, the -- Congress thought that it was advisable to provide confidentiality exemptions from FOIA of discoverability and reports of critical infrastructure information in order to encourage the private sector to share information with the government that may be very important to confronting the homeland security challenges that we face as a nation.

The way that the Act works, I'm now on slide 21, is that the Department of Homeland Security will receive information that's submitted through a special process to the Department. There are special rules that will then govern its confidential treatment and handling. And the Department of Homeland Security has announced that it plans to share, and I think it's begun sharing with federal, state and local agencies under special agreements, or rather it will shortly share, under special agreement this critical infrastructure information. The agreements are supposed to provide the same level of protection that applies under the critical infrastructure regs that DHS has, although in practice, rather than in theory, things can work out somewhat differently.

What is critical infrastructure information? It's defined in the Act as systems and assets that are so vital that their incapacitation or destruction would have a debilitating effect on the security, economic security, public health or safety of our nation.

And what sort of information is available for protection so that it can be kept confidential? Information about attacks, compromising or incapacitation of systems, including unauthorized access to virtually any communication system, so hacking incidents for example, information about the ability of any kind of technology or system to resist these sorts of attacks, compromising or incapacitation including security testing information, risk evaluation or risk management planning or audits.

And then finally, information about planned or past operational problems or solutions relating to critical infrastructure, including repair, recovery, insurance or business continuity issues. The range of situations where this Act can come into play are very very broad, but for example if you're government contractor and you're explaining to government some reasons and responding to some questions about your technology, you can use this process to protect certain information that you're supplying. Or if you're required -- if you are reporting to the DHS Cyber Security Unit a security problem and you don't want hackers to be able to get this information or your competitors to get this information, this sort of protection can really come in handy. There is a broad range of other contexts, but any time that you are voluntarily communicating with government about any of these topics to the Department of Homeland Security, this kind of protection can be advantageous, although as we'll discuss, it's not bulletproof.

Turning to slide 23, to obtain confidential treatment the information must be voluntarily submitted for a security purpose to the critical infrastructure information program manager in the Department of Homeland Security or any of his designees, and it must contain an express statement along the following lines. This information is voluntarily submitted to the Federal government in expectation of protection from disclosure as provided by the provisions of the Critical Infrastructure Information Act of 2002.

There's no reason not to use exactly this phrase. It's in DHS regs, and when you submit information that you want to be protected you should be sure that it contains this express statement. There's also a provision for providing oral information to the Department of Homeland Security. And if so, you need to follow up within 15 calendar days with a written submission of the same information using the same sort of statement.

So you can make in -- respond to a question over the phone or phone in information about a threat, and then if you follow up through this approved process you're supposed to get the same protection for your oral submission as you would for something that you've submitted in writing, if you follow up within 15 calendar days.

In addition, to obtain confidential treatment, the information must be submitted with a time certification, indicating that it is voluntarily submitted, that it is not being submitted in lieu of compliance with a federal requirement, that there's no requirement that this particular information be submitted to a federal agency, you can't bypass for example federal regulatory reporting requirements through this critical infrastructure information process. And then that information is not customarily found in the public domain because in that case you'd just be waiting government's time in submitting the information. In addition, you must affirm your understandings that false representations in these submissions may violate the False Statements Act 18 USC Section 1001 and be subject to criminal prosecutions.

What other benefits that you receive? First of all, before you know whether or not your application has been accepted, you will receive and whether in practice this will always operate within 30 days remains to be seen, but an acknowledgement of receipt within 30 days and get a tracking number. There is a presumption of protection of confidentiality while your submission is being reviewed and DHS may contact the submitter to request more information if the submission does not appear to qualify, and also give the submitter the choice to withdraw.

If you see that DHS is challenging or has questions about your submission you may prefer simply to withdraw it. It will ask if you prefer that information be maintained by DHS if it's not qualified for confidential treatment or destroyed per the Federal Records Act, and there is an exception for destruction if the information would be useful for law enforcement or national security reasons, even if you do request that it be destroyed.

In addition, the Critical Information Infrastructure Program can decide to change the status of a submission after it's been submitted if it comes to light that information shouldn't be protected, in which case you will hear from them.

Now, what are the protections that you enjoy if your submission has been approved -- this is on slide 26. the information will be specially marked. It's supposed to be subject to secure handling and transmission and the source, proprietary/business sensitive information is to be removed in any sort of alert to the public that's made or any sort of disclosure to a foreign government. So the fact that you were the entity that submitted the information shouldn't be known, at least if the information is shared that widely. So the identifying information will be stripped.

It may be disclosed, however, to state or local authorities and government contractors if they agree to meet all the requirements of the act. There's a specific requirement of no disclosure by contractors to subcontractors without prior written approval of DHS or of the submitter. There's also a requirement for no further disclosure by state and local governments if they get the information from DHS, unless the submitter of the information, if you've given the information, for example, to DHS agrees.

Furthermore, state and local governments may only use the information to protect or enforce their laws, although in theory if there were a violation of a law that was made available by -- if you've submitted information to DHS that was shared with state or local authorities and it indicated that you were in some way not in compliance with a federal or state or local regulatory requirement, they could use that information.

In addition, there's an exemption from federal and state Freedom of Information Acts so that the information can't be disclosed. However, state and local authorities, if they get the information from DHS may turnaround and request the same information from you. So there may be information that's of interest to them for their own security planning purposes then that they could then realize that you had information, they couldn't do anything with the DHS version that had been supplied, but they could go and request it from you.

There are some exceptions for investigations or prosecutions of crimes, disclosures to Congress or the Controller General, to any other employee within DHS, and there's also a whistleblower exception if it comes to light -- if the information could be used to show wrongdoing on the part of the government or the submitter. So that's the critical infrastructure information protection and it's something that is useful, although there's no guarantee of absolute confidentiality, and I've described some of the holes in it, but I hope it's helpful to you. Thanks a lot, Rob.

Rob Levin - *Moderator*

Thanks, Jim. We're going to switch gears for a second. Our final speaker is Deborah Rosenbloom. Deborah is a Vice President of The Cohen Group. Cohen Group is an international strategic business consulting firm headed by former US Secretary of Defense, William Cohen. Most recently, Ms Rosenbloom was the Department of Defense's policy adviser for homeland security responsible for developing and overseeing the Department of Defense's policies and programs in support of the Bush administration's homeland security strategy. Deborah will address the recent changes at the Department of Homeland Security and will also provide an outlook on the future of the homeland security market.

Deborah Rosenbloom - *The Cohen Group - Vice President*

Good, thank you very much Rob, and thanks everyone for listening in. Before I talk about the future of DHS and what we can expect or at least guess about, I thought it would be useful if we look back on some of the patterns that have become -- begun to emerge in DHS over the past 18 to 24 months on the procurement side that they have been involved with.

Before I turn directly to the lessons learned, let's take a minute though and talk about what we have seen by way of funding for DHS, and that can also help us in terms of understanding where the Department is going.

Initially, as everyone is aware, there was a great expectation that this new area of homeland security was going to be a gold rush on the power of a rise in defense spending. And indeed, federal spending on homeland security-related activities has gone up by about 14 billion in discretionary spending in 2001 to what has recently been approved at 35 billion in 2005. But it still remains modest relative to spending on Defense at the approved level of 402 billion for FY 05, Health and Human Services at 68 billion for FY 05 and Education at 57 billion for FY 05. The increases in DHS funding which have occurred are largely attributable to salaries and expenses of new law enforcement and aviation security personnel, as well as pass-throughs to the states and localities.

Procurement which has occurred has been largely on aviation security, as well as continued Coast Guard modernization. In fact, in FY 03, which is the last year we have rolled up numbers for, procurement was about 18% of the DHS budget and stood at $6 billion, of which 1.5 billion went to Coast Guard modernization and 2.5 to TSA for aviation security. The remaining money largely went to what we would call commodity items -- ammunition, fuel, guns and back-office technology support.

When we look at the spending pattern which has occurred in the Department's procurement, there were a few lessons learned for this point that we can draw. For those companies who have traditionally worked with DoD that experience can be useful in your approach to the DHS market, but in many ways it can obscure the procurement picture of what's going on at DHS. So we thought it would be useful to review a quick few lessons over the past 20 months to help direct future marketing strategies to the Department.

First, unlike DoD, there is no single Department-wide culture. In fact, it is very fragmented. While one might say there are distinct differences between the Air Force, Army, Marine Corps and Navy, the differences pale by comparison to the distinct cultures within DHS. You have communities together that share very different traditions and backgrounds, as well as, frankly speaking, different and distinct missions. Contrast the Emergency Response and Preparedness folks with those from Customs and Border and protection. Each directorate has its own culture and it is important to understand and absorb these differences. It is also important to look at whether it's a civil agency, law enforcement or one which is on loan from the intelligence community.

Second, in addition to diverse cultures, decision-making is highly decentralized. Each directorate is a decision nexus and there is very little if any integration across the Department. We do not see this changing the very near term.

Notwithstanding, Admiral Loy, as well as former Secretary Ridge's outstanding leadership in trying to bring the Department together, it has remained very much a confederation, and so for the foreseeable future integration projects will need to be

developed internal to the directorate. This reality commends a very decentralized approach to marketing to the Department, and also to develop customer intimacy at lower levels within the Department of Homeland Security that might otherwise be the case at other federal agencies. Third, like DoD, DHS has continued to show a tendency to rely on lead system integrators to help problem-solve and provide recommended solutions and to implement them as well.

What is starkly different from the Department of Defense is the kind of integrators that they are turning to. At Department of Defense there are those integrators which DoD partners with for the development and integration of weapons systems, such as Lockheed Martin, Northrop Grumman, Raytheon, just to mention a few, and there are those that they will use for back-office processes, such as BearingPoint, Accenture, and Unisys. We would be shocked to open the paper one day to see that Accenture was leading an integration project directly in support of a DoD mission, but that is exactly what is happening at DHS. Because of their lack of personnel, as well as the lack of knowledge regarding process management, DHS is relying increasingly on integrators that specialize in knowledge or process management.

With the notable exception of Boeing and Lockheed's early support to DHS on aviation security, DHS has placed greater emphasis on knowledge management and transformation process management over the technology. Whether this will continue will depend upon the new DHS leadership and what is occurring today within the Department.

Fourth, notwithstanding the Department's public pronouncements regarding integration and department-wide spending on management innovation and consolidation, DHS has been largely focused on operational requirements. Leadership attention and monies were expended in reaction to threaten levels and in direct support of law enforcement. This focus on operations has, in some cases, required leadership and management to focus away from putting in place centralized planning, budgeting and programming functions and centralized procurement.

Finally, the role of research and development is evolving at Department of Homeland Security in a way very differently from that at the Department of Defense. At the DoD there is a culture of long-term research and development in addition to ACTDs. At DHS, HSARPA acts more like a large ACTD, which focus on off-the-shelf rapid prototyping and quick field deployment. If you make it a habit of skipping DARPA in your custom calls, I would encourage you not to skip HSARPA and the broader S&T directorate.

Finally, for my final remarks before the question-and-answer period, I wanted to raise areas that we believe will be future focus for the Department of Homeland Security. In the near term, the opportunities we believe lay in bio surveillance, chemical, biological, radiological and nuclear countermeasures, Maritime Port security within US waters and territory, aviation security, notably in cargo screening, as well as information sharing, particularly related to communications with states and localities as well as interoperable communication.

Moving out to more mid-term opportunities, we believe that the Department will be focused on intermodal transportation, land border security and agro-terrorism. And an area which continues to have problems politically and certainly legally, but which we believe will remain very important, is predictive analysis and data mining. With that, I will close my remarks and certainly happy to answer any questions.

QUESTIONS AND ANSWERS

Rob Levin - *Moderator*

Thank you Deborah and thank you to all of today's speakers for providing a brief overview of the homeland security landscape. We're now going to take questions from the audience. If you haven't e-mailed your questions in, again, the e-mail address is Homeland@PiperRudnick.com. David? David Mendelsohn?

David Mendelsohn - *Piper Rudnick - Partner in Homeland Security and Insurance Practice Groups*

Yes?

Rob Levin - *Moderator*

Hi, it Rob Levin. You spoke earlier about some pretty heavy responsibilities, fiduciary responsibilities and business continuity planning. As a corporate counsel who reports to a busy CEO, my question is how do these folks deal with this risk? How much preparedness is enough when youre trying to account for something that really isn't foreseeable? And how could a company avoid wasting its limited and precious resources to deal with these issues?

David Mendelsohn - *Piper Rudnick - Partner in Homeland Security and Insurance Practice Groups*

Well, it's a reasonable question because my remarks might be taken as being somewhat alarming -- they're certainly not intended to be. The answer of course is it depends. It depends on the company and the business in question and what they perceive to be the critical aspects of their business operations that might be at risk. I think one sensible approach to dealing with this issue is to engage in a complete or comprehensive assessment of risks that your business may be exposed to in the event of a breach of security or in the event of some catastrophic or disastrous event, whether it's terrorism-related or weather-related or blackout or whatever it might be, and then to make assessments based on that information.

Remember, the directors and officers ultimately are not going to be found liable for making bad decisions, they're going to be liable if they fail to make informed decisions. And it's also clear from Caremark and from the business judgment more generally that what's called unconsidered inaction is not going to be protected. So conduct the assessments and then see what information you get as a result. I don't think -- and then react accordingly. I don't think companies have an obligation or a responsibility to say well, if there is an exact repeat of 9/11 what do we do or if there is a chemical or biological attack in the city of Detroit, what impact is that going to have on our business? I think the focus for management has to be a little more sensible in the sense that I think they focus on what are the kinds of events or consequences of events that could disrupt their business.

So if there is a blackout, what does that mean? If there is a fire, or an explosion, what will be the consequences that flow and then devise plans, both security plans, business continuity plans, that address the consequences of disasters rather than trying to figure out every possible nasty event that might be perceived as a possibility given this new age in which we live.

Rob Levin - *Moderator*

Thanks David. A question for Jay Westermeier. Jay, can you give us some practical examples of what companies are doing to improve their information security and cyber security programs? And sort of on a practical level, how can they integrate legal controls and procedures into the program?

Jay Westermeier - *Piper Rudnick - Partner in Business and Technology Practice Group*

Thank you Rob, that's a very big question, a very big undertaking to try to do that. But basically what we have found is that if you conduct an audit of the security function in terms of how legal practices and legal controls can fit in, we often find that the disaster recovery and the business continuity plans and the other agreements that have been entered into often don't constitute an integrated security plan and there really needs to be an effort to make sure everything fits and works together.

And one of the things that we have developed is the whole concept of legal battle plans. We believe in this time and space that we don't have the luxury necessarily of bringing lawyers in to look at a cyber incident and to determine what kind of reaction should be done. And companies really need to think through the whole process of providing legal responses and make sure

that these responses are integrated with their other responses and so that you have off-the-shelf battle plans that could be adapted and modified and put into action very very quickly.

This day and age, security should be something that is reflected in all contracts that the companies enter into -- employment agreements, supplier agreements, vendor agreements, outsourcing agreements. We're starting to see more and more service level agreements with respect to all aspects of security and this needs to all be integrated because security has become a priority matter and the contracts the company enters into need to reflect the importance of security.

So it's a new world out there with respect to security. I mean there are many things that the legal department can do in terms of employment agreements, information policies, e-mail policies and -- to try to provide the legal framework to support computer security, to make sure that the company has in place legal remedies that they can pursue to mitigate losses and reduce particular losses from computer security incidents.

Rob Levin - *Moderator*

Thanks Jay. Kevin, question for you. Question that is near and dear to my heart. With respect to the SAFETY Act, we know that only a few applications have been granted. Can you give us some insight as to why that is? Whether the SAFETY Act process is really serving the intended effect and whether you see any improvement in the process that will allow companies to more quickly obtain the types of protections that the SAFETY Act is intended to provide?

Kevin Mullen - *Piper Rudnick - Partner in Homeland Security Practice Group*

Sure. Let me put that answer first into context. The SAFETY Act itself was enacted in November 2002. The Department of Homeland security's interim rule and their application kit was issued October 2003, so in the two years since the statute and the 13 months since the rule and the application kit, these are the statistics that are most recent for the Department of Homeland Security. What they call pre-applications, the short form, at the beginning of the application form, they've received 150 or so of those pre-applications.

They've received about 50 full applications, which is a more rigorous process for the applicant. They've received four or five -- it's unclear to me whether the fifth one has been granted yet -- approvals for those applications since effectively the 13 months that the process has been in place. In my opinion I think most people would agree that's an underwhelming set of statistics there, and if -- most people who are following this legislation would've predicted something 100 times or 1,000 times higher in terms of the numbers. So from that perspective, it's a little bit troubling when you ask the question is the congressional intent being satisfied here? I think probably not.

Now, what are the reasons for that? I think there's probably two. One is that companies are taking a kind of wait-and-see attitude, so they're waiting to see how the Department of Homeland Security will administer the process. They're waiting to see what kind of companies will submit applications, what kind of companies can get approval, how many approvals will be forthcoming, what will be the practical approach to applying the various criteria to the applications. As a result of all that waiting and seeing, there's nothing to look at. I mean, you have 150 pre-applications, which are not of much help in providing a track record, and only 50 applications. So with the track record of four or five approvals we haven't learned much.

Now, the second reason for this is I think an exaggerated emphasis by the Department of Homeland Security on one particular criterion. In the statute there are seven criteria that are identified for approval, and those criteria address the effectiveness of the technology for mitigating or detecting the terrorist threat, the real risk of such a threat, the reliability of your technology, the safety of your technology and the clarity of whether there is in fact excess liability for the seller. That is, you can't get suitable insurance coverage.

One of the criteria, criterion number four, in simplified form, says but for the SAFETY Act would the seller market and deploy this technology? And in focusing on that particular criterion, many sellers who have existing products already on the marketplace, but who are faced with this potential excess liability, are number one, reluctant to provide applications because they think they don't satisfy that particular criterion; and number two, I think the applications that are in process are being bogged down in the dialogue between the Department of Homeland Security and those companies in determining whether that particular criterion is satisfied.

The other part of your question, with regard to what to expect in 2005, I think, first of all, we had a new and designated secretary for the Department of Homeland Security awaiting confirmation, Bernard Kerik. There's an opportunity here for industry to perhaps suggest some streamlining to the process, suggested a more realistic flexible approach to this criterion number four, I think we can be hopeful.

Mr. Kerik was part of the emergency preparedness and the response effort in New York City, so I would think that the SAFETY Act and its purposes would resonate with him. Industry surely is exercised -- there's a number of trade associations that have focused on this, so I'm hopeful that we're going to see a much more practical use of the SAFETY Act process in 2005.

Rob Levin - *Moderator*

Thanks Kevin. Just as a follow-up, in practical terms, what kind of technologies or products fall under the SAFETY Act protections so that our audience can understand whether they are sitting on a product that might be eligible for this kind of protection?

Kevin Mullen - *Piper Rudnick - Partner in Homeland Security Practice Group*

The products that are closest to the core of this kind of coverage are products that are sold for homeland security purposes. Now, they don't have to have that as an exclusive purpose, but it should be one of the core purposes of the particular technology.

For example, your company has biometric technology. That's in the core of many Homeland security solutions. There are other security type products, both in terms of physical security, bomb detection, x-ray equipment, one of the applicants who received SAFETY Act coverage, one of the four that we know about, had a product that in essence was a water-powered product that would cut into and help with rescue operations. So water-powered cutting device that was used in rescue operations. So the closer you are to the core of the homeland security activity then the closer you are to satisfying the eligibility requirements. And also, and not coincidentally, the closer you are to exposing your company to extreme liability in the event of a terrorist attack.

Rob Levin - *Moderator*

Thanks. Debra.

Deborah Rosenbloom - *The Cohen Group - Vice President*

Yes?

Rob Levin - *Moderator*

Can you elaborate a little bit on what we can expect from the new Department of Homeland Security leadership?

Deborah Rosenbloom - *The Cohen Group - Vice President*

I think overall, Rob, it's very early to tell. I mean, there certainly are ways to look at the previous leadership and background and experiences which Bernie Kerik has had in New York and in other places. But equally important will be to watch over the coming weeks and months as to the transitions which will occur at the Undersecretary level.

Those individuals which will be heading up the individual directorates such as the Information Analysis and Infrastructure Protection, Science and Technology, Emergency Preparedness and Response, Border Transportation and Security, because in many respects the overall management piece with respect to the Department and some of the priorities we can expend to be set at that level and whether they will change dramatically from what we have seen I would argue likely not in that near term. I certainly think one of the areas that the Department will continue to focus attention on is certainly maritime and related issues.

We can also expect to see renewed effort with respect to management and consolidation efforts amongst the individual directorates. And so I think as we watch the different moving pieces over the next month or so, it will be as critical certainly to watch who becomes the Deputy Secretary as well as which of the Undersecretaries leave and with whom they will be replaced.

Rob Levin - *Moderator*

Thanks. Just a follow-up, and this may be appropriate for Debra, Kevin, or anyone else, can you give us an update on the status of the 9/11 legislation, which is the Intel bill which we've all been reading about? And can you briefly summarize what it contains as regards potential business opportunities for businesses in this area?

Deborah Rosenbloom - *The Cohen Group - Vice President*

Well, the status of the bill we certainly can speak to that. It passed the House last night and is before the Senate right now as we are speaking, with the expectation that they will vote it out this afternoon and then the bill will go shortly to the President for his signature. And it's certainly everyone's expectation that given how involved the President has been over the past week or so with respect to it, notwithstanding work that was done previously, that he will sign that and we will move forward with many of the reforms which are outlined in the bill, some of which ultimately will become the law, certainly.

Some of the key areas to look for and to review are ways in which some of the agencies will now have new programmatic responsibilities -- the consolidation of those -- as well as where some of the new requirements will be coming and where some of that requirement definition process will be done. By and large, however, I think what you're going to be seeing is you know consolidation and increased focus on consolidation on the policymaking, if you will, as opposed to any radical changes in programs at least in the near term.

Rob Levin - *Moderator*

Do you expect that we'll see an acceleration in some of these programs?

Deborah Rosenbloom - *The Cohen Group - Vice President*

Quite possibly, although the reality is it'll take time for -- I would expect to see greater change, quite honestly, reflected in latter part of 2005 and early 2006 than now because it will take quite a while with the stand up of the new NID and a consolidation of that organization before they will really be in a position to change radically the programs and policies which are currently being done at the existing agencies. So for the near term I do not expect to see radical change but certainly in the latter part of 2005 and the beginning of 2006 absolutely.

Rob Levin - *Moderator*

Bank Debra, and again, thanks to all of our speakers. If you had a question and did not hear your question answered, please note that a Piper Rudnick attorney will be sure to get back to you within a week. Also, should you need any further information about Piper Rudnick's homeland security practice, please visit www.PiperRudnick.com.

Thank you to the panelists and the audience. We hope that you found this Web cast informative and helpful for your practice.