



Compliance With the SAFETY Act

Compliance With the SAFETY Act

MARNI CENTOR: Hello, everyone. The Association of Corporate Counsel and SmartPros Legal & Ethics welcome you to today's webcast, "Compliance with the SAFETY Act."

[The instructions provided here were intended for attendees of the live webcast when it was originally broadcast.]

Our presentation today will be given by Brian Finch, a partner with Dickstein Shapiro LLP. And now, I'll turn it over to Brian.

BRIAN FINCH: Thank you, everyone. I appreciate your time for joining us today. As mentioned, my name is Brian Finch. I am a partner with the law firm Dickstein Shapiro in Washington, D.C., where I head the firm's Homeland Security Practice. We specialize in all areas related to homeland security, so well beyond the Department of Homeland Security, including the Department of Defense, Department of Transportation, Health and Human Services, state and local government and international partners, as well as private sector partners. And I am actually joined today by one of our private sector partners, Michael Crane, who is the executive vice president and general counsel of IPC International, which is one of the largest providers of security forces to commercial, retail and commercial office building spaces throughout the United States. As mentioned, today's topic is the SAFETY Act. SAFETY Act is a liability management tool available through the United States government, specifically the Department of Homeland Security, that is very significant in the way it can help manage any entity's liability that could arise out of a terrorist event.

To start with, you need to examine the legal environment before 9/11 happened. Pre-9/11, terrorism was remote in most people's minds. It was not something that we dealt with on a regular basis. It was typically only viewed through popular media, and the United States fortunately at that time had only a passing familiarity with acts of terrorism. Come 1993, the United States unfortunately had one of its first major encounters with terrorism with the bombing of the World Trade Center building in New York City.

For those of you who might recall, terrorists—Islamic terrorists—brought a truck into the parking garage area of the World Trade Center, and detonated a large ammonium nitrate bomb, resulting in significant damage to the World Trade Center complex and unfortunately some casualties, including fatalities. Arising out of that event, there were a number of claims that were brought, and the first set of claims that were brought were against the manufacturers of the fertilizers that were utilized in the act of terrorism. As many people might know, ammonium nitrate, which is standard agricultural fertilizer, when mixed with other common chemicals or elements, including diesel fuel or other accelerants, turns into a very powerful explosive. And as a result of that common knowledge, claims were brought against those manufacturers, and as you can see here from the slides, alleging a number of defects: negligence for failing to design, manufacture and/or sell a less detonable product; products liability design defects because the fertilizer was unreasonably dangerous or defective; and there was a failure to warn customers and others who might encounter the fertilizer, to let them know that it was, in fact, a dangerous tool and could be perverted into a terrorist weapon.

What happened with those initial claims was that the court dismissed those liability claims, holding that it was not reasonably foreseeable that terrorists in these cases would have utilized the fertilizer to make bombs. And in particular, as you can see from the slide, the court was pretty explicit. They said, “No jury could reasonably conclude that one accidental explosion 50 years ago, one terrorist act in the United States nearly 30 years ago, and scattered terrorist incidents throughout the world over the course of the last 30 years would make an incident like the World Trade Center bombing anything more than a remote or theoretical possibility.” So the claims against the fertilizer manufacturers in those instances were dismissed. And again, that was the mindset pre-9/11, that terrorist activities were unforeseeable, unknowable, and certainly shouldn’t result in liability for entities that were somehow involved in the terrorist attack, whether they were the victims or they provided a product that was somehow utilized in the course of the terrorist event.

Similar claims were presented following the 1995 bombing of the Federal Building in Oklahoma City. Again, we all remember that very unfortunate incident where a large ammonium nitrate bomb was utilized against the Federal Building, resulting in over 160 deaths, innumerable injuries and nearly complete destruction of the Federal Building. Again, since it was a fertilizer bomb, claims of negligence and strict liability against manufacturers of the fertilizer used by the two terrorists who created the bomb were brought. And again, much like the 1993 World Trade Center claims, the court, in this instance, also found that the fertilizer manufacturers had no duty to the plaintiffs to prevent them from harm, that the products themselves were not unreasonably dangerous or defective, and—this is very important, which is why I have it bolded and highlighted—the intervening actions of the terrorists destroyed any proximate cause arguments the plaintiffs might have had establishing some form of liability to the defendants. In other words, in an application of common sense, the court here held that when a terrorist takes a product or somehow defeats a service—and in this case, a product—and transforms it into a weapon, or utilizes it as a weapon in a terrorist incident, the actions of the terrorist are considered to be the linkage to liability. And anybody who provided the product or provided the service, they were not going to be held liable in these particular instances. So the actions of the terrorist destroy the proximate cause, thereby allowing the defendants to escape liability in these particular circumstances. So again, you look at the legal environment—legal liability environment—pre-9/11.

These decisions left defendants with a large number of defenses, including no specific duty to protect plaintiffs from terrorist activity. Terrorist attacks were an unforeseeable event. The actions of terrorists are so unique that they sever any possible liability links to the defendants, and claims regarding negligent design and/or manufacturing were unlikely.

So, moving forward, into potential terrorist events, there were a number of good defenses available to potential defendants to say, “If something, God forbid, should happen related to a terrorist event, we have a number of defenses at our disposal that should insulate us from liability.” And that’s a fair assumption and, I think a good number of people would agree, a good outcome from these types of events. Common manufacturers of goods or products shouldn’t necessarily be held liable in the event a terrorist takes their product and transforms it into a weapon to cause chaos, destruction, death, for political motivation or otherwise. This simply doesn’t seem to comport with common sense and gave a good reasonable measure of value and confidence to manufacturers of these products to say, “We can continue to deploy these products

without worrying about potential terrorist liability. Besides, what's really going to happen on a large scale within the United States that relates to terrorism?"

Well, you turn to 9/11. 9/11, as we all know, was an incredibly unfortunate series of events resulting in catastrophic personal losses and losses to property. Again, following the attacks of 9/11, plaintiffs filed a number of claims against defendants. Here, in this case, it wasn't just the manufacturer of a particular widget. It wasn't just the fertilizer manufacturers. Now you had it expanded to a far larger audience—far larger spectrum of potential defendants. It included port authorities, security companies, landlords, building owners, airframe manufacturers and others.

Utilizing the well-established precedent that occurred pre-9/11, defendants sought dismissal, saying there was no duty to plaintiff, and defendants could not have reasonably anticipated the actions of the terrorists. I think that's a particularly relevant point, too. With respect to the lack of foreseeability and the lack of anticipation of the actions of the terrorists. I teach a class on homeland security law over at George Washington University Law School, and we have a class dedicated to the 9/11 Commission Report. And one of the major points we draw out of our students and highlight in that reading is that the government was chastised for a lack of imagination when it came to its pre-9/11 mindset, meaning that they didn't anticipate, they didn't visualize, they didn't rank high enough the possibility that terrorists would utilize breaks in the security system at airports and in our transportation system to commandeer an aircraft and turn it into a large-scale suicide cruise missile. That was a failure of our government to protect against 9/11, and this is a trillion-dollar apparatus that has hundreds of billions of dollars and hundreds of thousands of personnel dedicated specifically to combating not only criminal activity but terrorist activity. So if they couldn't have reasonably foreseen the actions of terrorists, why should a landlord? Why should a port authority? Why should a private security company? Why should an airframe manufacturer, who does not have those types of resources, nor is it expected to have those types of resources, anticipate the actions of terrorists?

Well, that would be common sense. That's not what happened with these decisions. Here a court, federal district court in the Southern District of New York, found that the actions of the terrorists were, in fact, reasonably foreseeable, and that a duty could have been owed to the plaintiffs, allowing it to move forward to evidentiary hearings and eventual judgment. The court, in fact, issued a rather stinging rebuke specifically to Boeing. Boeing had argued in part, based upon some of the claims that were asserted against it related to its cockpit doors, that they could not have foreseen that a terrorist would hijack an aircraft and turn it into a human-guided cruise missile. This was not reasonably foreseeable, and so there should be no liability on the part of Boeing. Well, the court specifically rejected that argument, and as you can see in the fourth bullet point, they said that the danger of a plane crashing as a result of a hijacking was "the very risk that Boeing should have reasonably foreseen." So that leads you to the uh-oh moment when it comes to Boeing.

So, how does this get even worse? Because it always does. You turn back, once again, to the 1993 World Trade Center attack. Now, I mentioned previously that claims by the Port Authority itself were dismissed against the fertilizer manufacturers and others, and they were found not to have any duty to the plaintiffs. They were unforeseeable events, etc. This was not the case when other defendants—those who had lost lives or suffered injuries as a result of the 1993 World Trade Center attacks—sued the Port Authority. There, the state courts in New York upheld the

decision against the Port Authority. There, they found that the Port Authority was, in fact, aware of the threat and was required to take reasonable mitigation steps against terrorist activity.

Think about it. The government was chastised a few years later for not having any imagination, but yet they are going to hold the Port Authority itself potentially liable, and actually liable, in this case, for terrorist activity and for failure to take reasonable mitigation steps.

Now, if you know anything about what happened in the 1993 World Trade Center bombing, you might sit back for a moment and say to yourself, “Well, let’s hang on for a second here.” The Port Authority in this particular case had some interesting challenges and some not necessarily helpful facts, shall we say, to deal with. And that included the fact for a number of years, vulnerability assessments and security assessments were conducted at the Port Authority, specifically at the World Trade Center, to examine for potential terrorist threats.

Some of those risk assessments even came out with recommendations that included imposing stronger controls at the parking garage because, under one scenario that was posed to the Port Authority, a terrorist could take a panel truck, load it with an ammonium nitrate explosive, bring it into the garage, where there is no checking for any devices [or] any criminal activity; the only entrance and access controls were for money purposes, to pay for parking. Terrorists could take this truck, park it in the garage, light a delayed fuse, walk out, and several minutes later an enormous explosion would rip through the garage, and if parked in the right place, potentially topple the towers.

Well, that’s exactly what happened in 1993. Ramzi Yousef and his cohorts obtained a rental van, mixed their own explosives, utilizing ammonium nitrate, drove it in to the parking garage at the World Trade Center, parked it, lit a delayed fuse, and left the area, aligned for the large scale explosion. There were some positives coming out of this, namely that, number one, they parked it in the wrong area. If they had parked it 300 feet in a different direction they would have taken out one of the main support columns for the World Trade Center tower, causing it to collapse immediately and perhaps even collapse into the adjoining tower. That didn’t happen. What also didn’t happen was that the 250 pounds of cyanide that were contained in the truck didn’t release into the HVAC system as they had intended, resulting in a chemical attack as well, but instead it was consumed by the explosive power and the fire resulting from the ammonium nitrate attack. Still, even with those rather devilish details, you have to put that aside. And you can’t think in the context of, “Well, we’re not going to ignore facts like that.” That’s not really the precedent that one needs to worry about when it comes to the World Trade Center and the Port Authority litigation.

The court sustained the verdict against the Port Authority by finding that notice of potential terrorist attacks was the appropriate standard to apply. And by that, the court meant that a defendant is on notice of potential terrorist attack when a defendant knew or “should have known” that a terrorist attack was possible. Sit back and think about that for a moment. “Knew or should have known.” There is a good number of people in large metropolitan areas who own iconic facilities—large structures that are visited by large numbers of people on a regular basis—that know they are potentially under a terrorist attack. Some people, post 9/11, ignored the second half, “should have known,” and they did that by deliberately avoiding vulnerability assessments and security reviews and saying, “Well, if I don’t know about it I am not necessarily

going to be held liable. I am not creating an evidentiary chain. I am not creating discoverable documents to show that potential terrorist threats were brought to our knowledge and we ignored them.” So no actions were taken.

What this Port Authority case does is that it eliminates that defense. Under the “should have known” standard, now it’s very easy for a jury to say, “Listen, you owned a large real estate building in a major metropolitan area. You should have known, by that simple virtue of the number of people coming in and out, that you are under a potential threat of terrorist activity.” Let’s even take it a step further. Your area—it could be near a large chemical facility that’s regulated by the Department of Homeland Security—it’s near an important government building. You live in an urban area that has been identified as high risk by the Department of Homeland Security, freeing up grants from DHS to local law enforcement in order to help them improve security in that region. Any one of those areas is an example of satisfying the “should have known” element of this test. So a lot more entities—a lot more companies, real estate holders, etc.—they are no falling in this category of “should have known.”

So once you are on notice, what must you do in order to help find yourself in a position where you can successfully defend from liability following a terrorist event? What you need to do is: You need to take “reasonable mitigation steps.” And here, “reasonable,” as defined by the New York courts, means any step that could previously have been considered burdensome, adding additional bothers: security cameras, hiring guards where you normally didn’t have guards before. Or it could even involve circumstances where the most stringent of mitigation measures suggested in the course of a vulnerability assessment would be considered “reasonable.” To put it another way, there is no way to figure out what is reasonable in the post-9/11 environment and the post-Port Authority decision environment.

Now we’re in a situation where almost anything could be considered reasonable. It’s not just doubling your guard force. It could be anything from doubling your guard force to quadrupling the number of cameras to conducting regular security assessments, evacuation drills, storage of antidotes, etc., etc., etc. So there’s a lot you need to do, and some things that are obviously reasonable, but the problem remains that you have no confidence that any given step or set of steps will be sufficient to be deemed reasonable in a court of law.

So that leaves owners of these facilities in a very difficult liability situation. So the question you’re then have to ask yourself is: OK, why are plaintiffs going to sue me? I mean I am not the one who detonated the bomb. I am not the one who pulled the trigger. I am not the one who released the anthrax. Well, there’s some pretty simple reasons as to why you’re going to be held liable.

First of all, it’s going to be impossible to recover from terrorists. Think back to a situation a few years ago. We all remember the unfortunate story involving Daniel Pearl, a journalist who was executed, for lack of a better term, in Pakistan by reputed members of Al Qaeda. A lawsuit was brought by Daniel Pearl’s widow against Al Qaeda, a dozen reputed terrorists and Pakistan’s largest bank. That suit was quickly withdrawn because no one had bothered to answer any of those claims. And no one had bothered to answer the initial filing of the claims against them. I also think it’s important to note here, too, that if we were able to find a process server that was able to track down Al Qaeda and its leaders in Pakistan, that’d be rather embarrassing for the

United States government, too. So your success on any number of levels in a lawsuit against terrorists, ranging from simple, appropriate serving and process, is not going—there's no level of confidence in that, much less whether these terrorists are going to respect the system and show up in Manhattan to file a defense in these cases.

Similarly, state sponsors. Are you going to be able to recover from state sponsors should there be an act of terrorism? They certainly have deeper pockets. Take, for example, the 1983 bombing of barracks in Lebanon. There, there were linkages drawn to the government of Iran. Suits were filed and in absentia a \$2.65 billion judgment was levied against Iran for the benefit of the relatives of the 240-plus military personnel killed in that bombing. However, as the judge himself noted, that this was going to be a symbolic ruling. There are nearly 1,000 plaintiffs and it is unsure how they are going to recover, since Iran still, to this day, is estranged to the United States, denied responsibility for the attack, and, once again, did not even respond to the lawsuit. So you have a moral victory. Which is not unimportant, but at the end of the day, justice is not going to be served in the form of a monetary recovery from the terrorist activity.

So that leaves the obvious, and why people are on this call today. Security providers and property owners—they have the deep pockets. They are the ones who are the most attractive targets for plaintiffs in the context of recovering dollars. What you also have to keep in mind here, too, is that strong recommendations exist when it comes to preventing terrorism. Think back to the reasonable mitigation and the notice steps that I mentioned out of the Port Authority [case]. The New York Police Department this summer issued its Engineering Security recommendations document. And in that document, it detailed security recommendations by tier, including for perimeter security, building design, access controls, screening, monitoring, emergency preparedness, air handling, and a number of other areas.

What does this do? This functionally sets yet another high bar that will likely have to be met in order to manage liability. So reports like this, which are becoming increasingly common, are out there. And once again, plaintiffs, if they are searching for a way to establish liability, they'll look at a document like this, they'll run through the tiered recommendations and say, "Was this done? Did you do this? Were you even planning on doing something like this?" If not, it's not going to be absolutely determinative for liability purposes, but it sure as heck is not going to look good.

The other thing to remember, too, is that litigation is going to happen. If you take a look at some studies that were done examining the motivations behind the lawsuits arising out of 9/11, you will find that the people who sued were not motivated by money. Remember, there was this 9/11 compensation fund. That was very generous and provided significant monetary relief to families of victims out of 9/11. However, not everybody looks at it that way. A number of the litigants who sued post-9/11 and opted out of the compensation fund considered it "hush money". They said people were being paid off not to go to court. Litigation was viewed as a way to get accountability. One respondent said, "I am looking for justice. I am looking for someone to be held accountable. There are people who did not do their job and I want to expose them."

If people could do it again, more said they would have opted out of the victim's compensation fund and pursued litigation. One person said, I felt "dirty" after taking the money out of the compensation fund.

And, in addition, if you look at it from the defendant's perspective, it's not hyperbole. The legal bills for some of the entities involved in the 9/11 litigation have run into the hundreds of millions of dollars. Some of that relates to insurance, but an awful lot of it relates to the civil action—the liability claims that are arising out of the 9/11 attacks. So, it can get awfully expensive, awfully quickly, in addition to the losses that you yourself suffered as a property owner or as a security provider as a result of the terrorist activity itself.

And then you think about the total picture. New York City and surrounding areas suffered tens of billions of dollars in losses. Somebody, particularly in this day and age, is going to want to recover that. Because of the continued threats of lawsuits, you are now seeing vendors who refuse to perform certain security work. That continues to this day. I just was speaking with somebody the other day about their potential liability related to a contract their company was pursuing and they said, “We walked away from the work. It would have been significant. It would have kept a lot of people employed, but we determined the liability potential was too great, and we could not justify making the investment in this work.”

I mentioned people who chose to participate in the litigation. They weren't motivated by money, but as you can see from the third bullet point, they got a lot of money. The people who participated in the compensation fund were receiving a little over \$2 million on average in compensation, while those who did sue, through a negotiated settlement, were receiving, on average, \$5 million. Two million times 3,000 people is a lot of money to begin with. Five million times 3,000, which is the number who were, unfortunately, killed by the 9/11 attacks; that gets really big.

OK. So now I have made everybody depressed. And you think to yourself, “What do I do now? How do I manage all of this liability, or do I just run out of the country? Do I not do any security offerings? Do I sell my business? Do I go into owning golf courses? What do I do?”

Well, you do have a number of liability mitigation options. You can procure additional terrorism insurance. That's possible, but it can get very expensive and only covers so much. We're all familiar with insurers' ways of avoiding liability and saying it wasn't covered by a particular clause within the insurance policy. So that's there, but not wholly reliable. What about indemnification and waiver of claims terms? If you can obtain them, that's great, but they are not going to cover everything, and obtaining them, as I'm sure many people are familiar with, obtaining an indemnification waiver claims is an awfully difficult thing to do, particularly when you are dealing with numbers as large as we could be talking about with respect to terrorism. Should I only do business with the U.S. government? Because they have liability protection and doesn't that help me? Well, sure. That can help manage some aspects of your liability, but it can also make you a greater litigation target. Why is that? Well, because if you are working for the federal government providing security services or technologies, the federal government can't be sued. But you can. And that's who they're going to go after. They're not going to go after the TSA for faulty screening. What they're realistically going to go after is: They're going to go after the manufacturer of the x-ray equipment, the explosive-detection equipment, because those are the people who can be sued.

Should you walk away from the security market altogether? That's possible. Some have done so. Some have sold off their security offerings, but many people cannot afford to do so. And this is

particularly true for owners of critical infrastructure or publicly accessible buildings. Do you get out of the real estate market? Do you get out of the sports and entertainment venue marketplace because of liability concerns? You could do that. But you also basically have no business left. So it's a very difficult situation that's being faced.

Fortunately, Congress came up with a very good answer, which is the SAFETY Act. SAFETY Act stands for Support Anti-Terrorism by Fostering Effective Technologies. [That's a] bit of a misnomer right away. The word "technologies" is misleading. It applies to both products and services; it's not just for widgets.

The SAFETY Act is part of the Homeland Security Act of 2002, the law that created the Department of Homeland Security itself. And what the SAFETY Act does is that it helps eliminate or minimize tort liability for sellers of Department of Homeland Security-approved antiterrorism technologies should there be a tort liability, third-party liability lawsuit after an act of terrorism. Now, these protections under the SAFETY Act can only be obtained by submitting an application to the Department of Homeland Security, and the protections apply even if the approved technologies are sold to commercial customers or if the act of terrorism occurs abroad, so long as U.S. interests are implicated; in other words, economic losses. Let's step back for a second and examine that second sub-bullet point.

When some people think about the SAFETY Act, they only think about it in the context of selling an x-ray machine to the TSA or an inspection device to Customs, or some software program to the Secret Service. They look at it as: Well, this is a defense that is available only to sellers of technologies to the government. And that's simply not the case. And I know Mike will address this later, but his company is a perfect example. These protections apply regardless of who your ultimate customer is. It does not matter whether it's public, private or even international. The way the SAFETY Act is written, it's intended to cover any and all sales, regardless of who the ultimate customer is.

Now, just as importantly, because terrorism is oftentimes an international concept, and sales of goods are often internationally driven, SAFETY Act protections apply overseas as well. They will most obviously apply in circumstances where it's an American airliner—American Airlines or USAir or Jet Blue flight that was in a different country and was attacked there. They also apply in circumstances where U.S. technology is sold abroad and used for antiterrorism purposes so long as U.S. economic interests are implicated, meaning that if there is an inspection device that is sold in, let's say, Europe, used for inspecting cargo containers, and it goes through one of those systems, there is an attack on the cargo container and it results in a loss of trade, whether it's a physical loss of cargo or through a disruption in trade, and there are claims abroad saying, "Well, we suffered business income losses as a result of this disruption in trade," the SAFETY Act can still apply in those circumstances, so long as those economic losses can be tied to the United States.

Now, another important point with respect to the SAFETY Act is its definition of the act of terrorism. Under the SAFETY Act, there is a three-part test to determine what is an act of terrorism. As you can see here, it's any unlawful act that causes harm, again, including financial harm, to persons, property or entities in the United States, or in the case of U.S. air carriers, U.S. flag vessels outside the United States. Here, (ii) causes harm, including financial harm, to

persons, property, or entities in the United States is where you have that international coverage. And (iii) uses or attempts to use instrumentalities, weapons or other methods designed or intended to cause mass destruction, injury, or other loss to the institutions of the United States. This is very important. And it's very broad. And again, the definition is read to include events that impact the United States. Well, what's really critically important to remember here, too, is that when we're talking about the SAFETY Act, it covers international acts of terrorism, domestic acts of terrorism, and even cyber-security events.

Cyber is very important to remember at this point. Cyber-terrorism, as we know from Google, from attacks on the U.S. government, from concerns about the energy industry, it's becoming increasingly prevalent. SAFETY Act applies in those circumstances as well.

Now, under the SAFETY Act there are two levels of protection offered, known as designation and certification. Under designation, there are a number of liability benefits that are offered. First and foremost, claims can only be filed in federal court. That's important. Being in federal court is, generally speaking, a good thing. Damages are capped at a level set by the Department of Homeland Security. If you are SAFETY Act approved, you get a letter from the department saying, "Your maximum liability for a terrorist event is \$10 million." And that's cumulative over a given year. So of there's three events and you get a total of \$30 million in damages awarded against you arising out of those various terrorist events, your maximum liability, not individually, but collectively, is \$10 million. There is a bar on punitive damages and prejudgment interest. There is also a reduction of claims recovery from collateral benefits, collateral sources, like insurance, etc. All those are protections you receive under the SAFETY Act at the designation level.

Now, under certification, which is the gold standard of the SAFETY Act, sellers also receive a presumption of immediate dismissal. So if there is a lawsuit against the seller of an x-ray machine or a security guard service that alleges that they were somehow negligent, defective in their provision of services, and the company is certified, like IPC International is, they have the ability to immediately walk away from that lawsuit. A claim will be filed against it and they'll file a motion to dismiss, saying, "We're entitled to a presumption of immediate dismissal." And absent a showing a fraud or misconduct in their submission of their application to the Department of Homeland Security, those claims must be dismissed.

One other important point to note: Under both designation and certification, any claims against customers—and this would actually be expanded to subcontractors, vendors, suppliers, licensees, etc.—all those claims are to be immediately dismissed. The only proper defendant in these lawsuits is the seller of the approved technology, whether it's the security guard service or the x-ray machine. Anybody else who has bought the system or has received it for utilization, they don't face any liability associated with the use of that technology. Very, very powerful benefit deliberately written in that way in order to prevent the SAFETY Act from being circumvented, and, frankly, a very powerful marketing tool for companies that have received the SAFETY Act protections.

So how does one pursue SAFETY Act protection? You have to file with the Department of Homeland Security, utilizing their application kit. Now, what is it that the DHS is looking for? They list a number of criteria, and they involve: What are you seeking coverage for? Is it the x-

ray machine itself? Or is it also the x-ray machine plus the maintenance services? How does the system work, and how is it provided? In the instance of a service, what's your standard operating procedures? What are your manuals? What are your policies? What are your procedures? For a technology, how exactly does it work? Where is the operator manual showing us how this detects explosives in a package? How do you know it works? What's your evidence of effectiveness when it comes to the particular technology? How will you make sure that it continues to work? Do you have an ongoing quality control/feedback loop to help determine that the product or service continues to be effective against terrorism?

Can you show that your products or services are repeatable? Are there documented policies and procedures that give the Department of Homeland Security confidence that, on a repeated basis, this system, this technology, this service can work? Is it safe? Actually, [this is] not all that of an unusual question these days, or an inappropriate one. There is a lot of debate going on right now about these full-body scan devices, millimeter wave scanners, back-scatter x-ray machines, CT scans, etc., to determine whether they're useful, whether they should be deployed, to protect the airlines and airport passengers.

Now, this is really an instance where the safety question comes in. Because a technology might do a great job of detecting explosives, but if you have repeated exposure to it, whether you're the operator of just someone who is being screened, could it increase your risk for cancer? That's actually something that's starting to show up a little bit with respect to some of these inspection technologies, and it is something the Department of Homeland Security will take a look at.

So once you have all this information and you put it together in the appropriate fashion, you submit your application to the Department of Homeland Security.

How does the application cycle work, once it's actually submitted to the Department of Homeland Security? Drafting of an application takes anywhere from 150 to 200 hours of personnel time. It's not an uninvolved process. It takes a lot of work, a lot of careful editing, and collection of supporting data in order to have it submitted to DHS.

Now, with respect to typical DHS review time, the department usually takes 30 days for what they call a "completeness check" to determine whether in fact they have all the information that they need in order to conduct the actual review. And then once that's been determined, the department then gives itself another 90 days to actually review the whole application packet itself. So overall, 120 days is the alleged typical review time. I will tell you that the department usually gives itself a bit of a break on the completeness check phase and will send back for more questions, and thus reset the clock for the actual review. So 120 days easily morphs into 150 to 180.

The science and technology undersecretary can issue an extension for the review. That used to happen somewhat more regularly; doesn't happen so much these days. So, I would say, generally speaking, from start to finish, you should expect about one year for an application to go through the SAFETY Act process. And by the way, you can group technologies together where appropriate, and you can submit multiple simultaneous applications to the department. It's just for each individual decision you should count on these time frames.

What happens when you get the actual decision from the Department of Homeland Security? You get a very nice letter—and when you're certified, a certificate suitable for framing—that provides the following information. The department says, "Here's the definition of the covered technology." In this particular instance, it'll say, "We cover the explosive trace detection device that you offer for use in airports and buildings. And in addition to that we're also going to cover your installation services, your maintenance services, your customer support services, etc.—whatever you get listed in that definition is where your liability protections extend. That's a very important point. Because you want to make sure you have as much in there as possible, so that you are as broadly protected as possible.

You also don't want, at the beginning of the SAFETY Act process, to ask for too much, because if you ask for too much, the department is likely to have trouble with the application and might say no or the initial go around.

The duration of the coverage. SAFETY Act protections are for a set amount of time for all sales or deployments in that time frame. By that I mean typically duration is five years. So let's say your SAFETY Act protections are from 2012 to 2017. Anything sold or deployed during that time frame gets SAFETY Act protections in perpetuity. It has a lifetime guarantee of SAFETY Act protections. If you don't renew your SAFETY Act protections, then starting in 2018, nothing you sell or nothing you deploy gets the liability protections of the SAFETY Act. So you have to be mindful of the duration of the coverage.

The decision details whether prior deployments are covered under the SAFETY Act. SAFETY Act can be retroactive. This is particularly vital for technologies and widgets, because some of them might have been sold in 2003, 2002, even pre-9/11. The SAFETY Act can reach back on those deployments and provide liability protection. Again, this is very useful for technologies, as well as risk assessments [or] engineering services that are previously done.

The department will also detail whether you have to procure additional insurance as part of your SAFETY Act approval, and if so, how much. You remember that I mentioned earlier, under designation, your liability is limited to an amount set by the Department of Homeland Security, and that limit is expressed in terms of how much insurance you have to maintain against acts of terrorism. So when I mention a \$0 million figure, you'll get a letter from the department saying, "You must maintain no less than \$10 million in insurance that will respond to acts of terrorism." And that's your maximum liability, when they say that \$10 million insurance number. I have seen it as low as \$1 million. I have seen it as high as a couple hundred million dollars. Definitely falls somewhere in between.

An important point to note here, too, is that when it comes to determining how much insurance you must maintain, the department is statutorily constrained, meaning that within the SAFETY Act statute itself, the department and Congress have established that you cannot be forced to purchase more insurance than is available on the world market, and you also can not be forced to purchase an amount of insurance that would unreasonably distort the price of your product or service offering. In other words, the department can come to you and say, "We're going to give you SAFETY Act protections, but we're going to ask you to maintain \$400 trillion dollars in insurance against terrorism." It simply doesn't work that way. Because there is no amount of insurance available like that on the world market, so that number would be thrown out.

Additionally the department might say to a small company, “OK, we’re going to have you get SAFETY Act protections, but your insurance amount has to be \$50 million.” Well, this could be a company that never has traditionally obtained more than \$2 million in insurance, it’s total revenue is \$3 million, and it could get \$50 million in insurance through a broker, but the cost of that insurance would be so high that they would have to pass it along to customers in a way that would make them uncompetitive from a marketing standpoint, and they wouldn’t be able to market the product with SAFETY Act protections. So you can then go back to the department and say, “It’s going to unreasonably distort the price of our product or service and so we want that insurance amount lowered.” And I have definitely done that. I have seen it lowered by 50 to 75 percent at times, from where they initially were.

And in addition, they also, when they look at your insurance program, they’re not necessarily going to capture all of it. We just had an instance where a company had a multi-hundred-million-dollar insurance portfolio specifically against terrorism, given some of the risks that they were concerned about, and the department came back after reviewing all their information and said, “You know what? We’re only going to have a third of your insurance power be required for SAFETY Act purposes.” So the client was very ecstatic about that, in part because now they actually made the SAFETY Act a revenue-positive activity. By virtue of going through this process and investing time and money into the process, they’re saving themselves, on an annual basis, hundreds of thousands if not millions of dollars. I think that’s something that chief financial officers and risk managers would really enjoy, having it backed up by solid, statutory defense.

One other important point to note is that if, unfortunately, you are unsuccessful in your application process, you can come back to the Department of Homeland Security as many times as you want until you get your liability protections. Now, whether companies have patience for this is a different issue, but the fact remains that if you are unsuccessful, you go back to the department and say, “Hey, where did we go wrong? What did we not provide that you wanted or what do we need to do now, going forward, in order to give you the confidence to pass along SAFETY Act protection?” The department will lay it out for you.

I will tell you, in essentially every instance that I have ever dealt with it, and I have had relatively few unsuccessful applications that I personally have handled, when it does happen, you go back to the department, you get your explanation, and in most instances you are able to come back and get it on the second go-round. And you can keep going as many times as you want. DHS might get annoyed with you, but that’s too bad for them. It’s their job to sit there and take the applications in and consider them, and allow them to go through the process to see if they meet the statutory criteria.

So how do you take advantage of the SAFETY Act, and how do you manage your liability? The first thing you do is: You file SAFETY Act applications. You look around, you see whatever you offer, you take a look at it, and you say to yourself, “OK, what has an antiterror application?” Where can I point to something and say, “Hey, that is useful against terrorism,” whether it’s my obvious offerings like security guards, or even if I own a facility, I have an entire division of my risk management and my security operations internally that are dedicated to combating a range of threats, including terrorism, those are all eligible for SAFETY Act protection. Consider security services, including physical security and screening operations. All those are eligible for

SAFETY Act protections.

I mentioned cyber. Cyber is another very important element that can receive SAFETY Act protection. Customers can weave SAFETY Act into procurements. I own a utility. And I am worried about my liability. How am I going to manage it, because I don't necessarily do anything internally that is eligible for SAFETY Act protections? Well, you can go out and require vendors to hold or apply for SAFETY Act protections, and say, "Hey, if you want to sell that fence, if you want to sell that camera system to us, we want you to go after the SAFETY Act."

There [are] plenty of technologies and services that you need to buy and are required to buy, whether by law or just by trying to meet the standard of care, that are already covered by the SAFETY Act that you can utilize and, as a customer, gain some immediate and important liability protections. And again, it's important to remember here, given all your options that I mentioned previously, the SAFETY Act is undoubtedly the best and probably the only way to manage your liability in a post-9/11 environment.

And just following up on the procurements, it's not unusual these days to see procurements mention the SAFETY Act. Numerous procurements are now being tied to the SAFETY Act approval process, including chemical companies that are regulated under the Chemical Facility Antiterrorism Standards Law that are requiring their security vendors to be SAFETY Act approved. The universe of customers demanding SAFETY Act approval is expanding—amusement parks, sports teams, entertainment venues, critical infrastructure owners, commercial real estate vendors, all of them are getting in on the act when it comes to SAFETY Act and saying, "If you have a service offering that relates to security, we want to see proof of SAFETY Act protections or, at the very least, evidence that you are pursuing the liability protections."

Now, here's a brief example of a procurement tied to the SAFETY Act. This is out of Los Angeles World Airports, LAX, and others. When they were seeking out security technologies, they included language in their RFP that said, "System implemented will be required to be designated and certified as a qualified antiterrorism technology under the SAFETY Act." [This is] straightforward, easy language to put into an RFP, but is a real discriminator for these folks in saying, "Not only do I get the liability protections, but let's face it, we have been through a fairly rigorous process to determine whether that entity has gotten SAFETY Act protections, so we might feel like we have some confidence that they know what they're doing if they have this SAFETY Act accreditation to their name." So why not go ahead and put it in here?

Now, what I am going to do now is I am going to turn it over briefly to Mike Crane, who is going to talk about why his company, IPC International, chose early on in the process to pursue the protections under the SAFETY Act. Mike, perhaps you want to explain for a minute what your thoughts were.

MIKE CRANE: Good afternoon. I am Mike Crane, executive vice president and general counsel of IPC International. I became aware of the SAFETY Act through legal publications and realized the liability protection it afforded for terrorism-related acts. I saw that the definition of the SAFETY Act protection included both products and services. IPC International has over 5,500 security officers, employees, providing security services at approximately 400 shopping malls nationwide and in Puerto Rico. I tried to complete the application myself and realized that it was

far too complicated, and that I did not fully understand or realize the focus of DHS and what they were looking for.

I hired Brian Finch because he worked on the drafting of the SAFETY Act law, and I knew he was the expert. It was the best investment that I could have made. Given the various warnings about the potential of a suicide bomber blowing him- or herself up in a shopping mall, I was extremely interested in anything that I could find that could limit or reduce our potential liability.

As Brian has indicated, the application process with DHS is extremely detailed and complicated. After the vetting and approval process by DHS, the award of the SAFETY Act certification to IPC indicates that we have an antiterrorism program in place that meets their standard. Certainly we have competition of other security guard companies that provide security services at shopping malls. When we obtained our certification, we were the first to have it among our competitors. Unfortunately that's not the case today, as they have all realized the enormous benefit of being SAFETY Act certified.

In addition, our clients, for the most part, also have become educated, and now require SAFETY Act certifications of its security contractors. What our clients realized is that by having IPC SAFETY Act certified, their liability exposure is also capped, based on our insurance limits set by DHS. If there is an act of terrorism that occurs at their mall, there is probably no doubt that there will be personal injury, property damage to both mall common areas and tenant spaces, guests, employees and customers. IPC's SAFETY Act certification limits IPC's liability exposure as well as our client's liability protection.

In summary, we are now in the process of gathering updated information for our SAFETY Act renewal application. It is something that is now mandatory for us to have in order to do business in our shopping mall environment. I would certainly encourage anyone who provides goods or services in the public arena where an act of terrorism is a possibility to consider getting SAFETY Act certification. Thanks, Brian. Back to you.

BRIAN FINCH: Great, thanks, Mike. We have an opportunity to answer any questions that might be submitted electronically, or we can certainly pursue them offline as well, if you like. But just to follow up on Mike's comments, and sort of wrap up as we are approaching the end of the program at this point, by noting that Mike's comments about why IPC pursued SAFETY Act [protection] ring really true these days, and are really growing. I mean, when we talk to potential applicants or just talk generally to people who have pursued the SAFETY Act, one of the largest motivators at this point is the fear that they're going to be caught lagging behind when it comes to their competitors. Because if one entity has it in a given field, then you can rest assured that that entity is going to promote that.

And it's important to remember that the SAFETY Act is not an Underwriters Laboratory accreditation from the Department of Homeland Security saying this product works, or it's Consumer Reports' best-value buy, but it is confirmation that it has met the criteria set forth in the SAFETY Act, which are not easy to meet. And so companies do promote that and customers are aware of that. And they realize that this is something that's very useful for us if we have that liability protection and that imprimatur of the SAFETY Act available to us. And again, if we can do something—if we basically have to purchase a service—why not get something that has a

significant liability protection attached to it that we otherwise would never have obtained?

And this is a comment that you will hear from the Department of Homeland Security themselves. And they will say, “This is a very powerful tool to manage liability, and that’s why we’re promoting it and why we are encouraging applicants to come forward, in all sorts of existing areas, as well as emerging areas like cyber-security as well.” So it’s a very important point for everyone to remember.

And since we are essentially at the end of our time at this point, barring any questions at this point, I’d just like to thank everybody for your time. You can see my contact information up on the screen. And again, if you would want to ask any questions offline, feel free to drop me an e-mail or a phone call. And if you have questions for Mike as well, I’d be delighted to pass those along to him, too.

So barring that, I’ll turn it back over to the ACC and thank everyone for their time.

MARNI CENTOR: Hi, Brian, and everyone else. We actually do have a question from the audience. And why don’t I read that. The first question is: How much longer will the pre-application take? And when do you recommend that someone undergo the pre-application process?

BRIAN FINCH: The pre-application process is an interesting one. It normally takes 21 days to go through the pre-application process. You have to be pretty careful with the pre-application process because, since it’s so generalized, it can lead to some misunderstandings with respect to what it is that you actually want to get protected from the Department of Homeland Security through the SAFETY Act. The department is all about, as I said, drawing a line between what you offer and what you don’t offer. And if you promote too much or you under-promote, or you surprise them with things after filing a pre-app, they can get a little bit confused. So you have to be careful what you submit. But that said, it should give you a good feel, too, with respect to what actually—where you are going with the application. And part of what we do, too, is—I’ve done over 130, at this point, applications out of 450 or so that have gone through the process. We certainly talk to people and tell them whether, out of hand, we don’t think it’s a good idea, or it’s an obvious application to pursue at that point. So I hope that answers the question.

MARNI CENTOR: OK, great.

[The instructions provided here were for use only by attendees of the live webcast.]

It does not look like we have any other questions at this time, so on behalf of the Association of Corporate Counsel and SmartPros Legal & Ethics, I thank you again for listening to today’s program. And have a good day.