INCIDENTAL PAPER

Seminar on Intelligence, Command, and Control

Taking Responsibility for Our Security
Robert P. Liscouski

Guest Presentations, Spring 2004
Carol A. Haave, Mark M. Lowenthal, Robert B. Murrett,
John C. Gannon, Joan A. Dempsey, Gregory J. Rattray,
Robert P. Liscouski, Arthur K. Cebrowski, Aris Pappas

January 2005

Program on Information Resources Policy

Center for Information Policy Research

Harvard University

The Program on Information Resources Policy is jointly sponsored by Harvard University and the Center for Information Policy Research.

Chairman
Anthony G. Oettinger

Managing Director
John C. B. LeGates

E-mail: pirp@deas.harvard.edu URL: http://www.pirp.harvard.edu
ISBN I-879716-89-5 **I-04-1**

January 2005

PROGRAM ON INFORMATION RESOURCES POLICY

Harvard University **Center for Information Policy Research**

Affiliates

- AT&T Corp.
- Australian Telecommunications Users Group
- BellSouth Corp.
- The Boeing Company
- Booz Allen Hamilton
- Center for Excellence in Education
- Commission of the European Communities
- Critical Path
- CyraCom International
- Ellacoya Networks, Inc.
- Hanaro Telecom Corp. (Korea)
- Hearst Newspapers
- Hitachi Research Institute (Japan)
- IBM Corp.
- Korea Telecom
- Lee Enterprises, Inc.
- Lexis–Nexis
- John and Mary R. Markle Foundation
- MITRE Corp.
- Motorola, Inc.
- National Security Research, Inc.
- NEC Corp. (Japan)
- NEST–Boston
- Nippon Telegraph & Telephone Corp (Japan)
- PDS Consulting
- PetaData Holdings, Ltd.
- Samara Associates
- Skadden, Arps, Slate, Meagher & Flom LLP
- Strategy Assistance Services
- TOR LLC
- TransMedia Exchange
- United States Government:
  - Department of Commerce
    - National Telecommunications and Information Administration
  - Department of Defense
    - National Defense University
  - Department of Health and Human Services
    - National Library of Medicine
  - Department of the Treasury
    - Office of the Comptroller of the Currency
  - Federal Communications Commission
  - National Security Agency
  - United States Postal Service
- Verizon

Taking Responsibility for Our Security

Robert P. Liscouski

April 15, 2004

Robert P. Liscouski was appointed as assistant secretary of infrastructure protection in the Department of Homeland Security (DHS) in March 2003. In this position he is responsible for programs that protect the nation's physical and digital assets from attack. Previously he served as director of information assurance for the Coca-Cola Corporation. His other private sector experience includes six years with ORION Scientific Systems, where he served as a vice president for the law enforcement division, developing and integrating software for the civilian intelligence community. Mr. Liscouski was also the founder and chief executive officer of PoliTech Research, Inc., a firm providing open source research and business intelligence services to Fortune 500 firms. Earlier in his career he served as a special agent in the Diplomatic Security Service of the U.S. Department of State and as a homicide and narcotics investigator for the Bergen County, New Jersey, prosecutor's office. He received a bachelor of science degree in criminal justice from the John Jay College of Criminal Justice and a master's degree in public administration from the John F. Kennedy School of Government at Harvard University.

Oettinger: Our next guest is another alumnus of the seminars. It is a great pleasure to introduce him. Bob, it's all yours.

Liscouski: Thanks, Tony. Going on the premise that less is more, we'll pack a lot into the next hour. We'll go right into the discussion here, but let me just give you the framework. You may or may not know what I do for a living, but effectively it's managing infrastructure protection. DHS has the responsibility to protect our nation's critical infrastructure. It is simple to say, but it is truly a complex task, because it's not what we do at the federal government level that matters; it's what we do at the national level, and there is a significant difference.

As you may be aware, approximately 85 percent of the critical infrastructure is owned and operated by the private sector. That means that DHS needs to go the extra mile to encourage and incentivize our private sector partners to work in close collaboration with their federal partners, to do what is necessary as it relates to protecting local infrastructure and, by extension, local communities. The challenge is not just the protection of nuclear power plants, the chemical sites, or the other energy-producing plants. It's soft targets. It's the gathering places of large crowds: it's the malls; it's the stadiums—anything that can attract large numbers of people can result in potential targets for Al Qaeda and other groups that will use various methods to inflict mass casualties. Again, it's at the local level that all these things have to be protected, so that means working with local police departments, first responders, and typically, again, the private sector in the context of their being the target set and trying to get programs around this.

As you know, there is not much history for DHS. We've been around for all of about thirteen months now. When I came to this job thirteen months ago there was nothing in terms of infrastructure within the department to rely upon to exercise any type of activity around this task. We had to build it. Some legacy organizations came into my office. Some came from the NIPC, the National Infrastructure Protection Center at the FBI [Federal Bureau of Investigation]. The Critical Infrastructure Assurance Office, CIAO; FEDCIRC [Federal Computer Incident Response Center], which was the sort of computer monitoring capability for the government at GSA [General Services Administration]; something called the NCS, the National Communications System; and something called the Energy Assurance Office came over to DHS as well. So we had various flavors of people coming in from different organizations, mostly with different experience and different cultures, and all geared now toward trying to leverage what they did before but doing it broadly across all the federal agencies for infrastructure protection. That's the first data point.

The second data point was that we were at war with Iraq within three weeks of becoming a department. We were facing some very serious threats in the homeland posed by various groups either in support of the Iraqi government at the time or just generally operating here in the United States. We knew Al Qaeda was still alive and well here in the United States. So we had some very real tactical things we had to do as we were forming ourselves as a government organization and coming up with a broad strategy for how we were going to implement that strategy. We were working on a very tactical level on the one hand and a very strategic level on the other hand, because we had to create programs that would build capability over the long term. We're still doing that and we're effectively managing those programs. That's sort of the backdrop of what we're doing.

With the formation of the DHS also came the first comprehensive effort to ensure the protection of our nation's critical infrastructure. Although the mandate to protect bits and pieces of our nation's infrastructure was scattered across the government under such organizations as the NIPC, whose primary mandate was focused on cyber and which had a nominal budget of about $6 million a year, and the Department of Energy, it was not comprehensive or coordinated. Today, however, the collective framework in which we're operating is vastly different from any that had been applied in government's history.

To give you an example of how complex and challenging this is, let me ask you a question. If you were looking at all sectors of the federal agencies that would have domain in this space, under what component of infrastructure do you think pipelines fall? Pipelines could be gas pipelines or oil pipelines. Just hazard a guess! The Department of Energy, correct? It's actually the Department of Transportation, but what is flowing through those pipes is directly related to energy. So we look at the juxtaposition of responsibilities versus a logical breakdown, and that's just one example of how some of this stuff can get pretty complex pretty quickly. We had to reconcile all those things, and we're still in the process of reconciling those responsibilities and trying to figure out how we can best execute them.

But when we talk about the framework, my point is that it's a risk management framework. It's not a total protection framework. We don't operate under the premise that we can protect all things at all times. In fact, we have a calculus by which we determine what we should be doing and we prioritize our efforts by the consequence of loss. The consequence could be a human loss, an economic loss, or impact on national security. That's how we're organizing ourselves at the tactical level. That risk analysis approach is predicated on the fact that we are not threat based. We can't do our work on the basis of threats. We have to do our work on the basis of vulnerabilities, so it's a fairly straightforward process.

The way we have divided it up can scale at the national level or right down to the individual company level. It's sort of a five-step program. The first part is that you have to identify the assets you need to protect. At the national level it's those things that are national security related. At the company level it's those things that might aggregate into an infrastructure component, or those things that might be part of your supply chain so you can do whatever you need to do to produce and stay in business. You have to understand what you have to protect.

Step two is that you have to understand what the vulnerabilities are and how those vulnerabilities can be exploited, where the gaps are in those vulnerabilities, and what the interdependencies of those vulnerabilities are.

Step three is prioritization. We have to normalize nationally. We have to create a normalized list of key assets and critical infrastructure, and it's diverse. Then we have to figure out how to prioritize that, because the city of Boston has a different list than the one we have at the national level. Now, why would that be? Well, we see things at one level of granularity, and they see things at a higher level of granularity that would add more fidelity around the list that we have at the national level. So, clearly, we need to normalize that and agree about the priorities against which we think we need to be executing.

Step four is putting programs around those activities, those vulnerabilities. Now, what's a vulnerability? A vulnerability is any weakness in an asset's or infrastructure's design, implementation, or operation that can be exploited by an adversary. For example, a tall commercial building with underground or on-street parking may be vulnerable to attack from a car or truck bomb, referred to as a vehicle-borne improvised explosive device. We saw this in the 1993 World Trade Center bombing and in the 1995 Oklahoma City bombing of the Alfred P. Murrah Federal Building. In this example, the vulnerability is that a building could be attacked by a vehicle bomb if appropriate protective measures such as bomb-sniffing dogs or vehicle barriers are not in place. So we have safety issues and security issues. The vulnerability could be a chemical plant, and if there were an explosion in that plant it could affect a significant population. It could be a nuclear power plant. It could be the water supply or the very diverse food supply. There's a "farm-to-fork" concept of how you have to protect the food supply chain and ensure that you can keep confidence in the food supply. So, those types of approaches have significant vulnerabilities in each of those areas that we have to try to remediate.

The fifth step in this process is the metrics, and there are two types of metrics. There are outputs, meaning activity that you can measure to see if in fact you're doing what you said you were going to be doing and you can assess the effectiveness of those outputs. Then there are outcome-based metrics. There is a little bit of difference in how we look at those things.

Typically, the government will look at programs from the budget perspective. Are you on target with spending your money in a budget cycle that will consume what you projected, or will you overshoot your budget goals, which will require you to look for reprogramming from other parts of your department or agency to meet your program needs? I don’t mean to be unkind about this, but it’s typically not geared toward the production of a thing that’s measurable in terms of a programmatic activity beyond making sure your contracts are in place and you’re burning the dollars you budgeted. Bureaucrats measure their performance on the basis of the dollars that they’re burning and how well they’re increasing their budgets over the following years. What we’re trying to do is a bit more entrepreneurial. It’s driven at the execution level to ensure that we don’t simply have things going on, but that they’re the right things going on at the right time to affect the output, which means lowering the vulnerability or lowering the potential loss in a catastrophic sense.

Now, as I pointed out, this is all in absence of any threat environment, because in a threat environment, when we layer threat on top of this particular type of activity, we have more clarity about how we can prioritize. From a risk management perspective we can put in the various factors relative to the threat, the likelihood that threat might be carried out, the vulnerability to the consequences, and then the programs we have to execute against to lower those threats. That’s precisely how we’re looking to do this across the national level writ large: the federal, state, local, tribal, and private sector environments.

The federal government has only so many resources that we can apply against this challenge. With that said, it is imperative that the private sector understand they have a critical role in providing their resources in conjunction with the government’s to protect local infrastructure. So the rational arguments we talked about at lunch are the ones that we’re trying to apply in this space to help them figure out what they do. Now, there is tension about doing that. The pushback I get from the private sector is oftentimes on the order of “If it’s really critical infrastructure, if it’s really germane to national security, why doesn’t the government do what it’s supposed to do to protect it?” We do; clearly we do. But if you’re the private sector and now you’re part of the bigger pie that makes up a critical infrastructure, I would argue that it’s your responsibility to maintain competitive advantage. You will maintain competitive advantage if you have the right things in place from a security perspective, holistically, that allow you to maintain your place in the marketplace while others in that marketplace might be disrupted by a terrorist attack, a natural disaster, or an all-hazards type of approach toward what might take them out of the marketplace.

Oettinger: Doesn’t that imply a rather uncommon long-run view? In the short run it would increase their costs, and absent an actual realized threat they’d be at a competitive disadvantage. How do you get around that?

Liscouski: It’s a tough argument. I’ll tell you how we’ll do it, and it’s not the byproduct. I’ll get to your question in a second.

We’ve got the threat world that we live in. You’re all familiar with the DHS alert system. We have five different categories: green, blue, yellow, orange, and red. Right now we’re at yellow. If where orange was immediately post September 11 represents an anomaly, then we’ve dropped down a little bit to our baseline yellow. If this is where we were a year afterwards, then we’ve raised the capability to protect ourselves to a level we didn’t have before. What we’re looking to do is to continue to raise that yellow bar in terms of capability beyond where we were ordinarily operating in the immediate post 9/11 environment—at orange—and build up capabilities sustainably over time. We’re trying to allow companies, local and state law enforcement authorities, and just generally the government, to increase their capacity to repel, deter, and protect themselves against an attack, because we keep pushing programs out there that raise our capability to do that. They’re long-term sustainable.

The reason is that whenever you do anything tactically, in the short run, the costs are significantly higher than when you can do it over the long term if you can find a rational way to build capacity over time. We’re forcing that to happen by continually raising the bar when we have an incident. Next time we go to orange, if we have to, there will again be a significant amount of resources applied to protect, but maybe not as many as we needed before, because we still have those things in place from the last time we went to orange. We continue to raise the bar, so to speak, in terms of capability to protect.

Now, to your point. The private sector that has to bear some of the cost burden, if they just had to do this in the short term, would immediately try to take the pressure off. What we’re trying to do is work with the CEOs [chief executive officers] from the top-down perspective to get them to buy into long-term investments in security; not just the locks, alarms, gates, and various weapons, but systemic programs that are geared toward human, cyber, and physical assets—the three legs of the stool that we believe is the holistic approach.

Student: You’re looking to companies to make them enforce safety measures themselves. In New York City and Washington, D.C., it seems there’s a credible threat and it could be in a business’s interest to protect itself, but how is that factored in somewhere else that really wouldn’t seem like a target?

Liscouski: The reality is that New York, Washington, Los Angeles, and other large metropolitan cities are different from Omaha, Nebraska, or other, smaller cities that don’t receive the same amount of money dedicated to them as a New York or a Los Angeles that’s in a higher threat category. First of all, there are a couple of different pots of money. Some of it is federal grant money, some is programmatic money, and some is state funds that will be geared toward meeting those types of threats and the things they have to do for protection. Federal grant money is allocated according to a formula, where again the calculations are based on the risk management approach. We will allocate greater sums of money to those higher threat areas.

Your question is really about how we get the private sector to do what they should be doing in areas where they ordinarily wouldn’t see a threat. It goes back to best practices. I’m a political appointee, so I represent an administration perspective on the one hand, and I’ll tell you that I also represent that as a pragmatic perspective on the other hand, because it can’t be about legislation. It has to be best practices. You’ve got to ingrain and bake in good security practices at the CEO and the business operating level for business continuity, disaster recovery, and all the things that would be germane to good business practices regardless of a terrorist threat or what the hazard is. You also have to bake in security practices on the basis of your knowledge of your threat environment. You don’t have to be a security expert; you just have to get good advice on what you need to be protecting against in the context of where you are. It’s not all things to all people, so you can take a measured approach toward what you think you have to protect and how to protect it.

We'd like to see a basic, baseline approach. Why legislation doesn't always work—and it typically doesn't work when you're trying to implement security programs—is because you only do what you get measured to do. If I legislate that all writing surfaces have to be flat and tan, but don't tell you what shade of tan, that's all you're going to do. Optimally, they should be twenty-eight inches high and all this other stuff. You are only going to spend money on those things you think you need to do versus those things that are going to contribute to a broader, holistic, and maybe more effective program. So we try to push a best practices approach, and try to work with the CEOs of major companies to offer leadership in this space and show that best practices work.

Somebody mentioned earlier the incentives from the risk management industry and that if you can prove you're following the best practice you should be incentivized by having a lower premium. I would also argue—and this might be something that's in the pipeline—that there should be tax breaks for spending money on certain areas. So there are a variety of ways to do this. Recognize that this is early thinking in the context of what we're trying to do for homeland security, but there are various ways to cut it.

Student: Still on the subject of cities and so on, you're basically giving the states what some people would call unfunded mandates and then you have certain states that may take it up a notch. For example, a while back we were talking about how in Boston they were searching more containers from ships than nationally. So if Boston becomes really secure, wouldn't a terrorist want to go somewhere else where it's less secure? How do you guys analyze that? Do you have a map and figure how to take that into account?

Liscouski: It goes back to a prioritization of the consequence of loss. I tell everybody that there's no quick fix in this. It's a very, very long road that we're traveling. We're talking about the highest profile we can in terms of priorities and consequences of types of events. If that means that there will be another event that might have an impact on 500 people, but not on 5,000 people, because we're taking certain measures to protect them, then I guess that's what we will end up doing. In the long run, we'll look into baking in the processes to prevent that from happening anywhere. One life is as valuable as ten lives. We just don't have the luxury of that approach right now.

What you're talking about is channeling. We do this overseas all the time, but overseas it's a finite target set. I've worked counterterrorism for a long time, and in the overseas environment it's a little bit easier because the target sets are more limited. If you're an American or if you're an American business, an American interest, a U.S. government interest, or a military interest, you know that you're going to be targeted. In other countries it's a little bit easier to see who is looking at you and you can set up certain programs that can detect that type of activity. Also, you can set up programs that will allow you to protect against certain types of activities, and you will channel them to other NATO [North Atlantic Treaty Organization] countries, G-8 countries, or other countries that support a coalition. Because you're a little stronger and the target is chosen by "I want a Western target. If we can't get the Americans, we'll get the Canadians," then if the Canadians are less well protected, too bad.

In the United States, if you channel somebody you're channeling them to another target in the United States. Is that an effective protection program? I would argue it's a protection program if you're channeling them from a chemical plant that might have an impact on over 50,000 people to a chemical plant that might have an impact on 500 people. Were you successful? If the metric is saving lives, this is an enormous success story. This is tough. This is not a public discussion about whose life is more important than someone else's life. This is about how you manage this in a risk environment where the threat is less than specific, the targets are ubiquitous, and the ability to conduct an attack is not necessarily technically difficult. So it's challenging.

Student: We've had a discussion in a couple of these classes about how much of the budget you should spend going after the terrorists. If the United States becomes totally secure you said they'd go after another country and you're vulnerable that way too. So, what is the right balance of going after them or focusing on security?

Liscouski: We live in a hard world.

Student: Could you describe your impressions of the interaction between the Department of Defense's [DOD's] NORTHCOM [Northern Command] and the DHS?

Liscouski: To be quite candid with you, we're still figuring out where the lanes in the road are for what NORTHCOM does and what DHS does. The Homeland Security Act divided the country into thirteen sectors with five key resource areas. The DOD has domain over the defense industrial base. That means they are responsible for the supply chain or value chain that allows the military–industrial complex to produce those things that are germane to national defense. Again, that's a pretty easy statement, but it's fairly complex when you try to divide up what that value chain is. The DOD has its definition of what contributes to that supply chain and it intersects with our definition of what's in the private sector. Sometimes there's overlap. Maybe sometimes overlap is okay, but we want to make sure that the communication to those overlapped communities is consistent. That's what we're trying to reconcile right now. So, NORTHCOM's responsibility for homeland defense would really be focused outside the border. It's going to be looking at the air, looking at the maritime threat, and then internally looking at what has impact on the defense industrial base.

This is not about DHS doing everything. Let me just put that on the table. Again, good government is not about replication of activity and efficiency in numbers. Good government is about coming up with coordinated strategies that allow all the different stakeholders to do what they have to do, make sure that they're doing what you want them to do and that you can measure it, and, by the way, make sure we get the products that we want—in this case, good protection. That is precisely what DHS is all about. It's precisely what my approach is in terms of working with the federal agencies that have responsibility in this space. Do I care if NORTHCOM is doing something that I want to do if they're doing it effectively? More power to them! The more we can shift responsibility to other agencies, especially when there is domain expertise where it needs to be done, the more we'll do it, because that's exactly what we should be doing.

Centralized government and centralized management of responsibility are ineffective. Anybody here from a business school would understand that. You distribute a capability. The problem is the farthest edges of your universe, not the closest edges. You cannot control things that are farther from your flagpole than anything you can reasonably expect to control. You've got to empower and get other people to do your work. That is exactly the approach the DHS is trying to take.

Here's what I told everybody. This is a private sector audience. The holy grail is information sharing. Everybody wants to share information. They want to get the right information at the right time to allow them to make the right decision about what they should be doing and when they should be doing it. That doesn't exist. It absolutely will never exist. Instead, you want to have reasonable judgment about what you should be doing, based upon pretty good information. To the private sector that means: do they share information with the government that ultimately might become publicly disclosed or might somehow jeopardize their privacy or their proprietary interests? How do they do it in a way that protects those interests? How do they do it and still get good security as a result?

So what I came up with is that if I can get confidence around the activities that are going on in the private sector and the state government (the private sector because I'm not looking to get my hands deep into what they do), I can answer the following questions: Do they understand the threat? Do they understand what they have to do? Are they doing it? Are they doing it well enough that they can measure whether what they're doing could correspond to the threat? If I can get confidence around all the answers to those questions then I don't care how they're doing it. It's almost like saying that if your goal is to learn something when you go to college and get good grades so you can get a job, will you spend twelve hours a day studying and get your "A"s or will you spend three hours a day, because you found a more effective way to do it? That's up to you. The end game here is the outcome: better protection, more fidelity around the answers so that we know what's being protected, how well it's being protected, and that we're countering the threat. So, it's a much different model than what most people wanted to gravitate to in the past: being sure that the government is providing everything they need.

Student: The argument has been made that there is no way to prevent all terrorist attacks. If that is the case, then is there such a thing as not doing your job well enough?

Liscouski: I was having a conversation with someone about how I define success. Do I define success by saying I've prevented an attack? My definition of success relates to my position, and my responsibility is to protect against all threats. There's a difference between prevention and protection. There's overlap, but there is a distinction. Prevention is everything related to law enforcement and intelligence that would interdict—take away—their ability to attack or disrupt. Protection has a starkly deterrent effect. It is to degree prevention, but there is a difference. It is necessary to recognize that.

In the context of not being able to prevent everything, will we be successful if one, two, or three events do occur? We fully expect that incidents are going to occur. You should not leave this room thinking that nothing is going to occur over the next year. The questions are where it is going to occur, and at what magnitude it will occur. That's the difference. We prepare for things to occur, and we prepare every single day for a terrorist event to take place. We don't know what kind of event, but we expect that something is going to happen. Is our strategy going to be a failure if an event occurs? No, it won't be a failure. It will be a failure if something occurs and we should have known about it, or we should have had the information to protect better, because it was a vulnerability that was obvious. In a year's time we can't remediate against all those things, and I can tell you right now that I'll judge that after it happens. I lose sleep a lot over that particular issue. When you go to bed at night, you know somebody might die the next day, because there are things you just can't do well enough to get the protection around there. No matter how much you work in this business, you realize it's a fact of life that something could happen at any time, and it bothers you.

Student: We discussed information sharing a little bit today. How do you strike the balance between sharing information and protecting information that you don't want getting out? For example, a year ago I saw a report on the news saying we've done a study and the U.S. infrastructure is most vulnerable in the following five areas. I remember thinking, "Do we really want to publish that report?" In your role, where you have one duty to help people understand where we're vulnerable but at the same time you don't want our enemies to understand where we're vulnerable, how do you strike a balance?

Liscouski: It's a tough balance to achieve. At the extreme I'd say I prefer to not make information available. I'll share information, and then it depends with whom you're sharing information. For instance, if you're all owners of critical infrastructure, I'd argue that you have a right to know the information you need about how to protect yourselves. If you're a local law enforcement agency, you clearly need to know what's vulnerable out there so you know how best to protect those areas and partner better with the private sector. There's no argument about that. If you're all critical infrastructure owners in the chemical sector, you'll want to make sure you know how best to protect yourselves.

Now, suppose you're private citizens and your mom and dad are living within a mile or half-mile radius of a big chemical plant. You want to know what impact a harmful release from that chemical plant would have on your family should a terrorist attack or a safety incident occur that results in a harmful release. First responders want to know that too.

So there is a balance. It doesn't mean you have to disclose all the vulnerabilities. You can disclose the impact or the consequences without necessarily having to disclose what the vulnerabilities are that lead to those consequences.

There are ways to share information and to get the first responders out there. I would argue that in a democratic society the first responders in local communities can put the right pressure on those sectors and those industries to get the right actions in place. It's happened already. Local communities have shut down chemical plants that pose dangers to them, because they feel they can't be protected. This is not an easy solution. Again, don't walk away thinking there is a black-and-white answer to any of this stuff. There is a balance, and we're trying to achieve that balance in the best way we can.

Student: On information sharing, can you discuss a little bit your relationship with the intelligence community? I know you guys are theoretically just consumers, but obviously you're generating all kinds of intelligence requirements that they maybe are not thinking about. What do the institutional barriers look like right now and how do you project the relationship there evolving in the next five or ten years?

Liscouski: That's a great question. If you've been following the 9/11 Commission results, I think you've got a pretty good picture of what the pre-9/11 law enforcement and intelligence communities looked like in terms of how we shared information (or for the longest time didn't share information), and what the barriers were. We have not broken down all of those barriers. Some of the cultural ones are still present. The technological barriers haven't been overcome entirely, but have been overcome significantly. The cultural barriers that existed in the past are changing due to many of the actions DHS is taking. I'm not taking credit for it, I'm just telling you that the advent of a new organization with a different mission forced a lot of those barriers to be broken.

It's still not perfect. For instance, the directorate that I work for, Information Analysis and Infrastructure Protection, brings together two parts of the same pie, or rather puzzle. The information analysis component is an intelligence component. We do intelligence analysis as opposed to collection; we're not a collection organization. We're an analytic organization, and we get analytic input and intelligence input from the entire intelligence community. We take that intelligence input and analyze the information. We map that information against our vulnerabilities. Our task is much more focused on targets, capabilities, and intent.

We get raw data from the intelligence community. We get processed and analyzed data from the intelligence community. The biggest thing we can do is develop a requirements package for the intelligence community so we can get more clarity around some of the issues, and that's what my organization is responsible for. I'm a daily intelligence devotee, so when I get intelligence we've got a whole requirements process by which we dissect that intelligence to figure out who has to do what and if they are doing it—that whole value chain.

The biggest thing we can produce is not just protective tactics and measures, but a requirements package to give to the intelligence community. We need to say, "Okay, tell us who is operating in these particular areas and has these capabilities," or "Give us more clarity around this type of threat or this particular type of MO [*modus operandi*] in terms of how that threat might be manifested." We keep pushing and keep trying to push more effectively. We have to get better at that. You see the arguments today in the paper about whether we need an MI5,[1] or a better intelligence function at a national level that speaks to the broad requirements differently from the way the FBI is doing it. It's related to our need for more clarity around case-level data—the tactical stuff that's going on. What cells are operating? Who is doing what? Who has the capability? What do they look like? How do they operate, and how do we map that into things that ultimately we can communicate so those at the target know what to do if this guy or this particular MO appears? There are a lot of ways to do it, but if you see certain things occurring, does that mean you're under a specific type of attack or tell you the timeframe of an attack? We're trying to push everything toward that type of approach. It's not working as well as it should, but it's working a whole lot better than it was in the past.

Student: As an analytical organization only, do you still find yourself having to muck around in the details of collection, because you have to decide if you're going to go into the intelligence

[1] MI5 is the United Kingdom's Security Service, or domestic security intelligence agency.

community's requirements system, or the FBI's, or some other domestic organization's? That must be a challenge.

Liscouski: That's a challenge. Pat Hughes, who is the assistant secretary for information analysis [IA], has that challenge.[2] He's pushing it hard himself. He's trying to come up with new processes that will allow him to push the intelligence community to where they've got to go. It's going to change over time. It's a work in progress, believe me.

Student: Is there any thought about why the CIA [Central Intelligence Agency] runs the Terrorist Threat Integration Center [TTIC] and why it did not go under the DHS?

Liscouski: It's a topic of discussion. I'm not going to be able to add much to it other to say that's a really good debate. TTIC was conceived and reported upon a year ago last January. The IA office, for all intents and purposes, was supposed to do what the TTIC does, and there is some debate yet on whether TTIC will remain independent or eventually wind up under DHS. Time will tell. At any rate, the intelligence community felt that they needed to have a fusion capability and an analysis capability as a separate stand-alone effort under the DCI [director of central intelligence], separate from the CIA, that would provide foreign intelligence for our analytic component that deals with the foreign threat. The difference is that it's not a domestic threat component. TTIC looks at some domestic threat information where there is a foreign nexus, but not at threats with a domestic focus. So that's the domain they're operating in. Then we get charged with sharing or blending this information with the FBI and making sure we understand what's going on out there that might be relevant to assessing vulnerabilities. There's a debate right now up on the Hill about where that really belongs.

Student: This may sound different in terms of the current political environment in the country, but could it be that we're actually jumping the gun? Maybe the 9/11 terrorists got lucky and didn't get caught. I don't want to devalue the lives of the 3,000 people who died that day, but in the Civil War we lost 18,000 people in one day at Antietam. I don't want to get into specifics, and I know you probably can't, but let's say that a nuclear bomb does go off in New York City and we're talking about a million or two million people dead. How is our country going to be able to handle that—like hospitals, infrastructure, and finances? If it happens tomorrow, or ever, is the DHS really going to be able to respond to a catastrophe on that level?

Liscouski: Again, DHS is the coordination point, but the action points are essentially at the local level. The first part of your question was, did they get lucky? If you've ever done anything complex—and 9/11 was a pretty simple but nonetheless still complex type of event—you'll know there is an element of luck. Only one of their guys got caught, and we didn't draw the conclusion about who he was until it was too late. It was a clear day, so they flew in VFR [visual flight restrictions] conditions all the way. Imagine if they tried to do that on a foggy day! What would they have done if they had gotten on the aircraft? I was in New York last night and this morning, and I can tell you that the they wouldn't have been able to see the Twin Towers, flying at that level at that rate of speed, with enough understanding of where they were going, because the

[2] Lieutenant General Patrick M. Hughes, U.S. Army (Ret.) was director of the Defense Intelligence Agency and before that served as the director for intelligence (J-2) on the Joint Staff.

weather conditions were unsuitable. So it was a beautiful, clear day. Did they check the weather reports before they decided “Okay, this is the day”? Maybe. So there was an element of luck there. A lot of things came together, as they oftentimes do, and it was tragic for the victims but lucky for the perpetrators.

In the big picture, were we in error or were they lucky? I would argue that the information coming out indicates there were things that we missed and maybe we could have gotten luckier ourselves on those. From an investigative standpoint I don’t think all the pieces were there to draw the connections that would have allowed interdiction at the level we needed to prevent 9/11 from happening. Maybe we can get lucky. I was a cop for a long time and I’ll tell you that in the cop’s world the harder you work the luckier you get. A big part of police work and law enforcement work is often luck—coupled with being good.

Now, what are we doing? The second part of your question was about what DHS is doing to coordinate our response and recovery capabilities. We are doing a lot. We regularly exercise incident management responsibilities, and we convene tabletop exercises and live exercises to prepare cities for disasters. They do these themselves as the first responder community. Are we at a level where we are able to respond to the kind of catastrophic event you described? Not entirely.

Student: Will we ever be?

Liscouski: Keeping it open-ended I would say yes, we would be. In the near term, could we respond to a catastrophic event that caused tens of thousands of casualties? Clearly, we exercise against that all the time. Will all things be in place to allow us to do that quickly enough? The events themselves will lead us to that conclusion. We’re building capacity there, and again it’s a long road. We need a network of doctors who could respond to a scene at one time. We need to make sure that we still have interoperable radios so that we can get people operating on the same frequency. All the factors that go into first response are difficult challenges. There is a lot of work being done. If it happened today, I’d say we could respond much better than we could have a year ago. If it happens a year from now, we’ll be better prepared than today. We are going to increase our capabilities continually.

Student: Did we ever have that capability during the Cold War, when a nuclear exchange, even an accidental one, would have been far more likely?

Liscouski: No. Do you mean evacuation plans? Turn your lights out, close your eyes, and get out of this building. Do you know how to do it? No. Why? Because it’s not ingrained into your thinking. The government is not going to tell you how to do that.

Oettinger: By the way, that’s an interesting point. The nearest safe exit is out this door and down the hall. The other exits are firetraps.

Liscouski: It’s a personal mindset. When you stay in a hotel, do you ever take a look at the fire exits?

Oettinger: Absolutely. I urge you all to do it.

Student: They don't want you to see where their stairs are.

Liscouski: Do you do it?

Student: I do it just for kicks.

Liscouski: Do you ever go to the fire exit and open it and see if it's being blocked?

Student: I usually go down the stairwell.

Liscouski: That's the way to do it. I do it all the time. Do you see if you can get back in and don't get locked in the stairwell? Do they keep the doors open so you can get back in?

Student: They usually do at the bottom.

Liscouski: Usually it's a security measure not to allow you in. It depends on what school of thought you come from. Do you carry a flashlight in your overnight bag so if you're in a hotel you know where you're going?

Oettinger: There's always one in my back pocket.

Liscouski: There's a Cold War guy right there!

Student: Did you guys plan that?

Liscouski: I'm serious. It's a mindset. If you don't adopt the mindset and act at an individual level, and you have to wait for somebody to come along and give you a helping hand, it is not going to happen. I was a cop for a long time, and I worked in an overseas environment for a long time. I've been in places and had things happen where I said "We should have planned for that" and we didn't. It just becomes ingrained in your thinking. It's not paranoia. It's just common sense.

Student: Exercises did take place during the Cold War.

Liscouski: What were they? Do you have any idea? "Get under your desk and take cover." I grew up in that environment.

Student: We haven't done that, though. After all, there's North Korea.

Liscouski: We need more civil defense and more consistent thinking at the local level about what your defense needs to be at the home level. We've lost that mindset. There was a gap between the cold war thinking of previous decades and today, and we have to regain that sense of responsibility. We actually have a campaign that is going back to thinking about what you have to do at a very personal level. In the New York Police Department [NYPD] they're getting people to think about stuff like that. They've got training programs on how to think about your own security. It has to be a locally driven response.

Student: What sort of oversight do you have as to how money is distributed for first response? I read that Alaska and Wyoming are the top recipients of this money, and maybe some fire department in Alabama or somewhere has no equipment to meet the possibility of an attack there. Is there any sort of oversight as to these independent entities?

Liscouski: Yes, but I can't speak about it with a great deal of knowledge, because that's not an area directly under my focus. There is a grant process, as I pointed out earlier, even for first responders. It's one thing in terms of programs that deal with protection. Then there are certain criteria for programs that deal with training and preparedness and response. The EP&R—Emergency Preparedness and Response—directorate, distinct from FEMA [Federal Emergency Management Agency], administers that. I'm not familiar with what their criteria are. Not everybody is going to get a fire truck or first-responder equipment. It is going to be based on population and where we believe the highest risk exists. Again, a U.S. government-driven grant program is not going to solve all of those problems.

Student: Maybe under the calculations that were set up Alaska deserved it most, but does anyone check over those grants?

Liscouski: We have to report to Congress on what we're doing. That doesn't necessarily mean that's a pure check. Clearly congressional interests can influence what they think are the requirements for first responders. They can drive things on the basis of earmarks but there is an oversight process. Believe me, we have plenty of oversight at the top level. Between Congress, the White House, the Office of Management and Budget [OMB], and lobbying groups out there representing the states, there is a lot of visibility into how things are being done.

Student: On the education program you were talking about for getting back in the right mindset, is the right way to do it just to get it out through the local level? Secretary Ridge got so much criticism initially when he said "Basically, duct tape your windows."

Liscouski: It must be locally driven. We can provide guidelines. We've got ready.gov. We've got informative Web sites. We can provide best practices.

Student: Did he get criticized because we no longer have that mindset and it's a different generation out there? If it were still the cold war, they might have said, "Oh, yeah, these are good ideas."

Liscouski: I think so. We go through these things. We have to do it. That mindset has got to change, but this is a societal issue, not just a homeland security issue. It's about how you protect your children. What do you tell your kids about Internet safety, and what does that mean? With child abductions occurring, how do you want your kids to act? What do you tell them when they're walking home from the school bus if they have to go a couple of blocks? It's that kind of thinking that we do well. We've got the DARE programs—the Drug Abuse Resistance Education programs—that tell you it's all about self-esteem. If you make a choice as an adult, fine, but a kid shouldn't be doing things because of peer pressure. Again, it's a mindset. We've got to engender that same thinking throughout the school system. It's a whole civics and civil defense approach.

Believe me, we really are looking at ways we can get better education and put in place the systems to provide that.

Student: How do you know it's going to work? There are a number of studies that indicate DARE really doesn't have any measurable impact on drug use. Are we going to go back to conducting public drills so that we can get really good at doing something that might not make any difference? How do you know, when you're spending money and time and resources on education, that it's actually going to make a difference?

Student: I think the problems with DARE are that addressing drug use is different from making sure the fire escape is accessible. People will respond differently.

Liscouski: You were talking about changing the mindsets of a lot of people. I think there are plenty of examples of how this stuff does work. You can choose not to do it and that's an individual choice. We as a government, whether a federal government or a state or local government, do have an obligation to educate people to make choices about what they do. I'm not going to force you to make a particular choice. I'm just going to tell you, "Here's a tool set. You're an adult, choose wisely. But don't come back to me and tell me we didn't do enough to protect you when we presented you with the choice to do it." You can't have it both ways.

Oettinger: On 9/11 many of the casualties in the Pentagon were due to smoke inhalation. If you go through many of the government agencies in Washington you now find smoke protection masks at every desk.

Liscouski: If you want to study security at a level that's more routinized with respect to this as a process approach, go to an engineering plant—someplace where they have hazardous processes going on. Go to a chemical plant or a nuclear plant and listen to the briefings you get when you walk in. Those aren't security related, they're safety related.

Everybody's thinking about what to do. I don't care where you are in the world: when you come into a meeting like this from the outside (and you're supposed to do a series of things before you get there from a safety perspective), it would be somebody's responsibility to brief you on what Tony just talked about: the exit plan, how you know when you have an emergency, what you are supposed to do in an emergency, and where you are supposed to go in the emergency. That's what they do. That's safety. I've been through this. If you don't begin to ingrain that thinking in people's minds then it's never going to happen. You have to make it a part of everybody's thinking and somehow make somebody accountable for its getting done. We can't take a blasé attitude about it.

What I get angry about—and I do get angry about this—is that I'll tell you what to do, and then you come back to me when you don't do it and suddenly you've become a victim. You had a choice. You're an adult. Choose to live your life the way you want to live it, but don't make yourself a victim. This is what risk management is about. I don't mean to be pontifical here, but you know the risks and you take them. You may not take them consciously, but you take a risk with every single thing you do every single day. I would argue that you should do it consciously. That way you can make your choice and have ownership over that risk.

Student: When corporations make these choices about risk they have limited liability. Companies are only worth so much and the executives are not going to be held personally accountable for losses. One of the problems of this approach is that it doesn't work for a corporation.

Liscouski: I don't think we know enough about how well it works with a different paradigm. Take consumer advocacy for a second. We talk about software liability. Suppose you're a software developer selling to the business community—and you're not Microsoft, where you might have dominance in the marketplace. Assume there is enough competition in the marketplace to allow customers to choose between a good software developer and a bad software developer whose products have a security hole. If I can educate the marketplace to understand what those differences are, choice becomes the dominant factor. If there is not a monopoly, so there is choice to be had, you'll take the choice. Volvo, even in an oligopoly, made its sales on the basis of safety. Why is that? Because people were worried about it.

Student: Right. There's a metric. You have a market for lemons in software security because people can't tell a bad product from a good one. With Volkswagen you have safety statistics. You can't have those statistics for security.

Liscouski: I think you can.

Student: You have to get them a different way.

Liscouski: You may have to get them a different way, but we've never collected enough statistics to be able to educate the consumer base about what's good and what's bad. It's a long approach, but I think we can do it. We've got to demand to do it. If we don't, we're missing an opportunity. If we're taking today's paradigm and saying we can't do it, you're right. We won't be able to do it with today's thinking. If over time we can push different thinking about this and have an expectation that we can change it, I'm convinced we can realize that expectation.

Responsible companies will do it. Companies do it all the time today. You just don't hear about them. One of the reasons is that it's based on protecting reputation, trademarks, and image. It's not necessarily based on looking at liability. The Coca Cola Company, for which I worked, is a great company, but what do they do? It's a marketing firm. They sell brown sugar water and a lot of other flavors. The point is that they are protecting their brand, which they spent billions of dollars developing, because the quality of their product has to be the thing that they are protecting. It's not just creating a sense of "I get a great feeling drinking Coca Cola," it's the quality and the consistency around the quality of products over time. When somebody attacked their reputation, trademark, or image they were very aggressive about protecting it. I don't mean somebody saying "Coke sucks." I'm talking about extortions and product contaminations, which happen all the time in the food and beverage industry. Companies aggressively counterattack and protect against that so that they can ensure they protect the shareholder value over the long term, regardless of what the liability might be for product contamination.

Student: Tylenol is a good example of that kind of tampering. There was that incident about fifteen years ago where they quickly took all the Tylenol off the market before the government did it.

Liscouski: Companies will do that, because they recognize that it's good business practice to do it. You shouldn't be too jaundiced about businesses engaging in this practice, because they will do the right thing for the right reasons. They might define the right reason as, "Hey, it's for the public good. I'll do it for that reason, but it also protects my market share, so I'll do it for that reason too. I can get a dual benefit out of this."

Student: Every person who has testified in front of the 9/11 Commission has said, "We all need to share information. Information sharing was the problem. We need to change the culture." They've been saying that for two years now—every single leader of every major intelligence community organization. The president even said in his press conference that there were still stovepipes. Why doesn't somebody just crack down from the top and say, "This is the way it's going to be"? Have you seen that kind of impetus from the president and the senior cabinet officials? Is anyone saying, "National Security Agency, you will now share everything you've got with CIA"? Who will work out the security details?

Liscouski: I see an attitudinal change. I really do. Everybody recognizes that we've got to do things differently. Tony has been operating in this space for a long time, and he can tell you that it's not just the 9/11 Commission that's forced this to the front. This has been a dominant theme for quite a long time.

I'm not trying to make excuses for anybody. It is hard. It's not as simple as just throwing a switch and getting people to share the information, and it's not about not always having the right information. I think the common theme within the intelligence community is not that we don't have enough but that we really don't know what it means. The analysis part of what we have to do is really the hardest thing to break down. I would not argue that you're wrong. We need to continue to break those stovepipes down, but there are very legitimate reasons why some stovepipes still need to be maintained. At the end of the day, there is more of a reason why we need to have a better flow of information than not. But it's not about the flow; it's about analysis and it's about what that information means. That's the toughest nut to crack. To perform good, relevant analysis that allows you to come up with something that you can really act upon is something that people are still trying to figure out how to do. On the basis of open testimony (in this particular case on Al Qaeda) I would suggest to you that we still don't have enough good information that's going to give us specificity around what's being done.

Student: I don't doubt the technical and academic challenges of doing analysis. I guess I'm looking at it more from a sociological, public policy, bureaucratic point of view. You can look at the tenure or the budget of organizations, because they can protect their information, but the incentive is still for them to run to Congress or the president and say, "Look at what I did!" instead of sharing it with someone else and coming together for a better piece of information.

Liscouski: There's an element of that. The personnel system kind of reinforces the problems with sharing among different agencies. With the type of information you're sharing it's a hard nut to crack.

The problem we see in sharing counterterrorism information between the state, local, and federal communities is a good example. The NYPD has excellent intelligence capability. There's a highly competent group of people working there, and they really beefed it up after 9/11. They have excellent operational capability. The frustration is that sometimes they don't get all the operational information that would allow them to connect to things that are not just local to New York. They don't have a broad-based capability to collect information across the United States. They have to rely on the FBI to do that. The FBI will go out and collect national information, so the stovepipe is at the local level where things are really happening. You have incident data, not intelligence data. It's crime; it's local stuff. But stuff you collect on the street can turn out to be intelligence information after it gets collected and you realize what you have.

The Los Angeles Police Department is doing the same thing, and so are Seattle, Chicago, et cetera. They're collecting that information. They're not necessarily sharing all of it up the chain with the FBI. It's not as if there is a big vacuum cleaner that just collects the stuff on a daily basis. We've got joint terrorism task force scenarios that sometimes get that data and sometimes don't. It's a huge problem.

My point is that with what's going on in New York or Los Angeles you would think the FBI would connect those dots that need to be connected, but the FBI oftentimes doesn't have access to the data it needs to connect the dots. They may not have the wherewithal. There are cultural issues there. I don't know, Tony, if you want to say anything about this.

Oettinger: What makes this a difficult problem is twofold. At one end there are legitimate reasons for things being apart. One of the most persuasive ones is that there are different skills required for different kinds of intelligence gathering, just as there are different skills required for different schools and departments in a university or in a corporation. You get succotash if you try to squish it all together. Once you have this kind of specialization, there are going to be problems in sharing. That's a hard problem to avoid, because if you give up the advantage of specialization you do not necessarily make up for it by sharing nonsense. So that's legitimate.

Now at the other end—and this strikes me as a certain hypocrisy of the part of the members of Congress—the congressional structure is an important element in this. The intelligence community reports to any number of committees and so on that are jealous of their own jurisdictions and will not give up their authority, even in the face of our current problems. They love to pin the blame on the executive branch to protect themselves. That institutional problem is one that DCI Tenet and a couple of others have had the courage to allude to, but there were no reactions to it. So you have a number of very complicated factors working, from the purely self-serving to the unavoidably necessary. I've only mentioned two out of dozens of elements that enter into this.

Liscouski: Take away the classification problem for a second and just assume that all information can be shared with everybody. Assume we have a perfect system by which we can say, "Okay, there is no classification barrier." Let's just say there are the cultural, technical sorts of barriers that currently exist.

Let's go back to the New York example. The NYPD is protecting New York to prevent another 9/11. New York is high on the target category. Suppose another attack occurred there. You can look back and say, "It's happened twice before and was done by the same group." What do you think the NYPD mandate is? Their mandate is to do the best damned intelligence collection they can to interdict things that are going on within the bounds of the borough of Manhattan and the other four boroughs. Does that mean that the FBI is going to share everything with them that has a law enforcement perspective and might be germane to the bigger intelligence picture and have national implications? If the NYPD is taking down a cell in New York, because it might be operationally capable of doing something that would have an impact on New York, from an intelligence perspective would the FBI want to turn that operation off and maybe achieve a bigger objective at a national level? We have these discussions all the time. The FBI's responsibilities are at the national level. That doesn't mean they would let something happen in New York for the sake of the big national picture, but there's a national picture and there's the local picture. You find they compete all the time.

I've shared with you a mixture of an administration viewpoint and personal observation from working in this space for (I hate to admit it) almost thirty years. I could stand up here and give you all the things that we would ordinarily say: "Rah, rah, we're doing all this stuff and we're going to make progress." I'll tell you that in my heart I believe that, or I wouldn't be doing this work. I don't need to be doing it. I'm not a career government person. You come into this work at a political level. I've been blessed by doing this, because it's a tremendously challenging opportunity and I just happened to be in the right place at the right time.

My point on that, though, is that it's extremely complex. It's easy to make judgments on things when you don't understand the complexities. Don't get me wrong about this: there are formulas that might give you a risk management approach and say, "This is the right thing to do," but when you talk about human factors and a lot of the judgments that play into this there is no good answer. If we can hit an 80 percent solution, man, we're doing really well!

I'm not suggesting we're going to stop. To give you a good example, you hear about suicide bombings in Israel all the time. You don't hear about the ones they prevent. They prevent about 90 percent of them. That's a pretty good success rate. It's those few suicide bombers who get through the fence, or have support networks in Tel Aviv and Jerusalem, who still make the headlines. The government is not going to be able to prevent them all. Even for a state such as Israel, which is at war, knows who its enemies are, and knows where they're coming from—which is an extremely difficult thing to do—Israel has a highly sensitized society and a highly sensitized military and police complex. We don't at this point.

So, take away that this is a long-term problem. If you're working in this space, or even if you're not, you're all part of the solution. You have to understand that you've got to get people to adapt. Everybody's got a responsibility. If you go into the private sector and you have nothing directly to do with government, you've still got to take this responsibility with you. If you don't, we're going to be fighting this war for a very long time.

With that, I thank you very much for the opportunity to speak with you. I'll tell you something else: Professor Oettinger is a national treasure, and I mean that sincerely. He's been working in this area for I don't know how many administrations.

Oettinger: It goes back to Johnson.

Liscouski: I've been fortunate, because I've been mentored by him. I wouldn't be where I am today—and I might have to curse him for this—if it weren't for his guiding me and allowing me to make mistakes along the way as well. So I just want to thank Tony publicly for what he represents. He is a national treasure. Take advantage of that, because you've got a tremendous opportunity to learn from somebody who has been around this space, and whom presidents and DCIs have relied on for advice for a long time. So, Tony, thank you very much.

Oettinger: Thank you, and have a safe trip.

Liscouski: Good seeing you again. Good luck, everybody, I hope you all enjoy yourselves.

Acronyms

CEO	chief executive officer
CIA	Central Intelligence Agency
DARE	Drug Abuse Resistance Education
DCI	director of central intelligence
DHS	Department of Homeland Security
DOD	Department of Defense
FBI	Federal Bureau of Investigation
IA	information analysis
MO	*modus operandi*
NIPC	National Infrastructure Protection Center
NORTHCOM	U.S. Northern Command
NYPD	New York Police Department
TTIC	Terrorist Threat Integration Center

Seminar2004

ISBN 1-879716-89-5