Cybersecurity in Your Neighborhood: Why Public-Private Partnerships Matter

Jane Harman:
Good afternoon. Hello, everyone. Please find your seats. Well, so much for starting on time, something we've vowed to do, but welcome to the Wilson Center. I'm Jane Harman, director, president, and CEO, and this is a National Conversation of great importance and one I personally feel I have been living for the last couple decades.

Imagine the local power generation facility in your hometown. You know where it is because you drive by it every day on the way to work. It's got a fence and a few guards and it's safe, right? Wrong. That facility, like many others, is probably controlled by an automated system that monitors valves and cooling elements. That system, run by a private sector company, is connected to the Internet so that it can be managed easily. And that automated system runs on software that could have an inadvertent flaw in it, exploitable by hackers determined to cause us harm.

As a former nine-term member of Congress who chaired the Intelligence and Terror Prevention Subcommittee of the House Homeland Security Committee for some years, and before that served on our intelligence committee for eight years, I can tell you that this scenario has kept me and many others in Congress and out, up at night. It is very possible. But many members of the Congress and the public don't appreciate or even understand what our government, especially the Homeland Security Department, could do to help prevent cyber-attacks in the private sector or elsewhere. Many also, recently, are conflating this issue of cyber-attacks with what they've been reading in the newspaper about the NSA programs. There are big differences and maybe that will be explained today, maybe not, but for anyone listening in or in this audience in front of me, believe me, this topic has to be addressed on its own. And for those of you worried about compromising privacy, as all of us should be, we have many different issues to discuss.

I think that this is a reset moment for the Department of Homeland Security. Now that the President has released an executive order on cyber, and most of you know about that, I'm sure it will be explained, and has asked for

recommendations from the executive branch, we can help explain and help conduct conversations around DHS's important role in cyber. It's not launch cyber-attacks, something you may have been reading about in the newspaper, and it's not to defend us from all cyber-attacks, but it is a very significant role and it relies on an active partnership with the private sector.

I had a conversation the other day with someone on Capitol Hill. I'm going to reveal his name. He is Senator Tom Coburn. And I mention him because he's a Republican. I was a Democrat in the House. He's a good friend of mine, but that doesn't mean we agree on everything, but he has a very significant role on this issue given his senior status on the Senate Homeland Security Committee. And we talked about DHS. The Secretary hasn't heard about this. And Tom Coburn was very positive. Of course I would relate a good news story. But this is a guy you might not think would necessarily think that the Department of Homeland Security should be ground zero on parts of this issue. And he said – I have notes here somewhere because I don't want to misstate what he said – he said, "The process used to craft the executive order should be praised. It was inclusive and our government listened." He also said he was impressed by the DHS staff, some of whom are in the room – in this audience – looking right up at us, that he met with and that he will work for a bipartisan solution for legislation that could enable this process. And I think that message coming from Tom Coburn means a lot, and so I wanted to be sure everyone heard it.

Everyone in this room should know what the stakes are. Not just the little example I gave, but you will hear more in the panel that follows, or maybe you'll even hear more from the Secretary. I kind of think it's almost like the Israel-Palestinian peace process. We all know what the end needs to be, but we just don't know how to get there and how to get the parties there. So maybe we should lock the doors and bring food in and figure it out. The only missing ingredient is currently serving members of Congress, but maybe I'd get them to come down, as well.

Someone to keynote this panel -- the one to keynote this panel is the Secretary of Homeland Security, Janet Napolitano, whom I have known for decades and decades. She will tell you that, when we met, she had a perm. I have no recollection of this. But she was a rock star in politics

in Arizona, was U.S. Attorney, was Attorney General, and then was Governor twice, and then left to take on this job where she is now in her fifth year as the Secretary for -- of Homeland for the Obama administration. She will deliver keynote remarks and will be followed by a panel discussion led by NPR reporter -- fearless NPR reporter Tom Gjelten, whose reporting on this subject and related subjects I find stunningly impressive. And, no, I'm not going to mention that he's married to Martha Raddatz, the rock star broadcaster.

On our panel will be former DHS Secretary Michael Chertoff, former federal judge, former Assistant Attorney General, who I found when I was in Congress to be just an exemplary partner. And, Michael, our friendship has succeeded both our tenures in our old jobs, but Michael's first question always was, "What's the right thing to do?" not, "What party do you represent?" And I salute you for that, my friend.

And on this panel is Steve Flynn, who is co-director of the Kostas Research Institute for Homeland Security, Northeastern University. Or he's about to be that, maybe he isn't yet. But who has worn a number of hats and is superbly qualified to address this topic. And we also have a very able private sector representative, Frank Taylor, who is head of security at General Electric.

I'll just say one more thing. This National Conversation follows a lunch we had with DHS representatives and private sector representatives, and I urge that everyone be very candid about their views of each other, and some of it wasn't so pretty, but I certainly left that lunch very hopeful, and I'm sure you'll hear some summaries of the lunch. We at the Wilson Center want to use our convening powers and our expertise to advance conversations like this. We're looking for the best policy ideas to form action plans to solve the toughest problems. And I think that on this subject we have made a very good start today. So please welcome my friend with a different hairdo, but a phenomenal resume and a very wise mind, Janet Napolitano.

[applause]

Janet Napolitano:
Well, good afternoon, everybody. We're here to discuss a topic that not only is incredibly important, but is

fundamental to the role of Homeland Security in a number of ways. So I thought what I would do this afternoon is briefly sketch the threat landscape, talk about the President's executive order and the President's policy directive on critical infrastructure because that also comes into play, and lay out for you what is going on at DHS, some of which you may have heard in other panels or at other times, but to reemphasize the importance of this within the whole schemata of the Department of Homeland Security.

It's the third largest department of the federal government. It's the youngest department of the federal government. It covers a myriad of missions that were put together under one roof following the terrorist attacks of 9/11. And we have seen the department grow and mature very swiftly over the last 10 years since it was enacted. We just celebrated our 10th anniversary, by the way. Secretary Chertoff is here. He was the second Secretary. Tom Ridge was the first. I am the third. So you have, respectively -- I guess that makes me Thomas Jefferson, as I like to say. And Tom Ridge is whatever -- oh, I guess you're John Adams.

In any event, I only mention that because not only are we changing and growing very fast in some areas, but we've seen some things evolve over this short period of time. You know, when we started, we were concerned with terrorist plots and attacks similar to 9/11; terrorists taking over commercial airliners and turning them into weapons and using them to fly into buildings. Aviation attacks and plots have not gone away. Indeed, that has been a leitmotif of my time at the department. We still see them in number and sophistication. They continue to change. The sources from whence they come continue to change, but they remain with us.

But fast-growing now alongside is this whole area of cyber and cyber capabilities, cyber interconnectivity, cyber-attack. And how do we secure the country in the best possible way, while respecting privacy and civil liberties and all of the other values that we hold? That's really the challenge that's presented to us. And so we have been growing very, very rapidly in the cyber world. When I started, it was a fairly small element of the department. The department was engaged with other threats, but as we have grown and as that threat has evolved, that's probably

been our largest area of just pure budget FTE growth, is the whole cyber realm.

It's located in several areas of the department. A lot of it is in NPPD. The acting Undersecretary on NPPD is here with you, but it's also the Secret Service. It's ICE HSI. It's CVP for intellectual property. So throughout the department, we now have cyber units working on different aspects of cybercrime and cyber security. So one of our big challenges has been to organize ourselves internally to handle that, and the second is to really look at what are the areas that we're most concerned about. Well, we're concerned about the theft of intellectual property. We've seen a massive transferal of intellectual wealth from the United States to other countries. We are just filing now our intellectual property theft strategy with the Congress for the next year. But this has been an area of concern. And all the countries of the world need to be engaged in this and participatory in how do we have cyber connected world and protect the research and development that goes into the creation of intellectual property?

Cybercrime writ large. I think of these at crimes that are simply committed using the new technology, the social media, whatever, that's available now. It can be identity theft. One very pernicious area, of course, is child exploitation, sex trafficking, and the like. ICE HSI just took down a major, major operation involving that, facilitated by the Internet. It is cyber terrorism and cyber-attack, and I think this is what most people think about who are in this room, but there is -- no doubt that there is a continuum of those who seek to do us harm as a country, ranging from individuals to organized groups to even groups that you could depict as state or state sponsored, who have been and are willing to engage in attacks against the United States and our critical infrastructure using the whole cyber realm, which gives them a whole new set of ways with which to go after us.

What does it mean? Well, what it means is, as Jane was saying, that critical infrastructure like utilities could be subject to attack. Oh, and by the way, if you think that that doesn't have a cascading set of issues, if any of you live in the New York/New Jersey area during hurricane Sandy, and you saw what happened there when the power utility was down for a number of weeks and all of a sudden, not only did you not have electricity for people who live

in tall buildings, so that all of a sudden 15-story apartments had to be walk-ups, but you saw -- then you didn't have electricity to get fuel out of tankers into tanker trucks, into gas stations and the gasoline pumps, and then out of gasoline pumps into cars. So that whole cascading set of developments. So this whole idea of attacking critical infrastructure and the control systems that govern critical infrastructure we've seen from a mother nature perspective, much less a human actor perspective.

We've seen it in the financial services area, the banking area. It's been a very active area, particularly for distributed denial of service attacks. We've seen the energy sector. Many of you know what happened with Aramco, where you had not just a virus, but a destructive virus that was entered into the system that actually destroyed not just software but hardware.

So we have a range of things that we deal with as a department and we have core responsibilities now where protecting the Homeland is concerned. So what does that mean? Well, let me, if I might, just give you a brief rundown on what we are doing within the critical infrastructure ambit of the department, leaving aside the cybercrime realm for right now. We have the National Cybersecurity and Communications Integration Center, the NCCIC, which has been open now about four years. It has responded to almost half-a-million incident reports in that short span of time. It has released more than 26,000 actionable alerts to the public and private sector partners in that period of time. On that watch floor, we have different government representatives, different government agencies. We have folks from the NSA, we have folks from the FBI, but we also have private sector representation on the NCCIC floor.

We have the United States Computer Emergency Readiness Team, the U.S. CERT. Many countries, by the way, have now developed their own CERTs, and we now have CERT-to-CERT relationships. But to give you a sense: last year we responded to approximately 190,000 cyber incidents and issued 7,450 cyber alerts through the U.S. CERT. And that was a 68 percent increase over 2011. So that's why this area is so fast growing.

In industrial controls, we have an industrial controls system CERT, ICS CERT. One-hundred-and-seventy-seven incidents last year. Eighty-nine site visits. We have 15 teams deployed to significant private sector cyber incidents.

So this is not imaginary or something that's speculative for in the future. These are things that are ongoing right now. We are working very closely with the private sector. These kinds of partnerships are not new. We work with the private sector where the protection of physical infrastructure is concerned. But with cyber, we now have two guiding, fundamental documents that we work from: the President's executive order and the President's policy directive, the PPD, on critical infrastructure.

The PPD directs us to take a broader look at our mission in cyber in a couple of ways: one, to take an all hazards approach, and, two, to make sure that we include protection of our networks, but also resilience; the ability to recover, to get back up quickly.

The executive order on critical infrastructure has three pillars: protecting privacy and civil liberties, promoting information-sharing, and setting up a voluntary program to encourage critical infrastructure owners and operators to adopt best practices. Let me just stop right there on those three pillars. First, privacy and civil liberties, from the disclosures about the NSA and their programs. As Jane mentioned, this is a very different set of things. But you should know that in the Department of Homeland Security, we actually have a privacy office and a civil liberties office, and those are experts in those fields whose sole job it is to look at what we are doing from the outset to make sure we are building into what we are doing appropriate protections for personal private information and for any kind of intelligence that we gather. And so we consider those values to be paramount. It's part of the way of life that we are here to protect. So that from the outset.

Information-sharing. You know, when the legislation failed last year, and I hope the Congress will be able to come back to this, one of the things that failed was the command really for real-time information-sharing. This has been one of the key tensions, I must say, between us and the private sector. We can't do anything if we don't know, or

don't know in real time, what signatures you're seeing, what abnormalities you're seeing so we can make a judgment as to whether this is something that arises to an alert level, this is something that we need to be engaging others on, whether this is a small problem or a big Homeland problem. But without real-time information-sharing, we are already starting off behind the ball. That has been a problem. Part of the bridge-building we need to do is solve the information-sharing aspect of this.

And then, finally, the voluntary program of adopting best practices throughout critical industry sectors. It's very interesting in this area. This is going to be, at this point, an experiment, and a very important one, because where security is concerned, law enforcement or security, we normally don't depend on the private sector. We really view that as an inherently governmental function. We don't depend or outsource our national defense to the private sector. We don't depend or outsource our intelligence-gathering capability to the private sector. We don't outsource local law enforcement or state law enforcement to the private sector. That is, as I mentioned, an inherently governmental function. We are proceeding in a different way here, pursuant to the PPD, and what that is is for the private sector, working with us and working with NIST, to set the framework and the standards to have a system that creates a voluntary program -- not voluntary program -- voluntary way, voluntary set of incentives for owners and operators to adopt best practices and to change their practices to meet evolving threats.

I think -- frankly, I know that some in the private sector are suspicious about the Department of Homeland Security or any government agency's ability to fulfill its function under the PPD. I have some question as to whether the private sector is willing to fulfill its function under the PPD. If we can make this work and show that there is a vital, ongoing, strong partnership between our capabilities and your capabilities and needs, we will have succeeded in this experiment. But let no one have any question -- I think we're still in the experimental phase. We're still working with each other, testing each other, meeting a lot with each other. All well and good, but I don't think we yet have come to closure on whether this is an appropriate thing to have as a shared responsibility as opposed to an inherently governmental responsibility.

So I'm expressing no opinion on this right now, but I just want to set for you, as you think about this, the fact that this is really the first time in our nation's history that we've approached a major security problem in this way.

You have, I think, already this morning heard about the integrated taskforce, which is designed to help setup the implementation plan for the PPD. In April they launched a collaboration community platform on idea scale for critical infrastructure stakeholders and all interested members of the public to post and share public comment and feedback regarding how we strengthen our networks and how we better protect our resilience.

In the first 120 days since the issuance of the EO and the PPD, we've already produced a number of deliverables, including an analysis, along with the Commerce Department and the Treasury Department, of potential government incentives that could be used to promote the adoption of the cybersecurity framework. These right now are at OMB where they are undergoing an inter-agency review process, but the initial work already has been done.

We've produced the description of critical infrastructure relationships that illustrate how our current organizational structure can provide risk management support to owners and operators and make it easier for them to collaborate with us. What does that mean? It means we've shared with you how these big, complicated departments are organized and what the portals of entry are so you know where to get help and where to provide ideas. We've supplied instructions on producing unclassified cyber threat reports to improve the ability of critical infrastructure partners to prevent and respond to significant threats.

Let me pause a moment here. I said unclassified. Let me put a bookmark down. I think one of our challenges, quite frankly, is to increase the capacity of those who are owners and operators of critical infrastructure to receive classified material and to receive classified material on a real-time basis. So the information sharing challenge goes both ways. It goes from private companies into us, but also us at the unclassified, but particularly the classified level, to you.

We have produced procedures for expansion of the enhanced cybersecurity services, the ECS program, to all critical infrastructure sectors to provide for greater cyber threat information-sharing, and we have provided recommendations on incorporating security standards into acquisition planning and contract administration to see what steps can be taken now to make existing procurement requirements more consistent with your cybersecurity goals. What does that mean? It means that we have to incorporate thinking about cybersecurity when we're purchasing IT. And, likewise, the same needs to happen with the owners and operators of critical infrastructure. What are the security needs, how do you maintain and sustain them?

NIST, which is part of the Department of Commerce, the National Institute of Standards and Technology, continues to develop the cybersecurity framework. That is due in October. So there's a lot of work that's been going on these last months, ongoing throughout the summer. Significant engagement by the private sector. And next up for us will be deliverables on the public-private partnership evaluation and cyber-dependent infrastructure identification. What does that mean? It means that under the PPD and EO it is the responsibility of the Department of Homeland Security to identify what is the nation's core critical infrastructure. What are we talking about? Who is included there? And we do that form a risk management perspective. What kind of core or what kind of infrastructure -- should it be taken down, should it be rendered inoperable -- would have a set of cascading impacts similar to what we see when an electric utility goes down for a period of time.

We need to, in this case, develop situational awareness capability for critical infrastructure. We need to update the existing national infrastructure protection plan, the NIPP. And we need to develop critical infrastructure performance goals that link to the NIST framework. So the goals are basically how to the what. You know, how are we going to get there? What is the framework that we all together seek to achieve?

So this is a very active process right now and it's fast-moving. This is a very aggressive timeline when you think about when the policy directive and executive orders were issued and when we are responsible to have the framework and to have the performance goals set, the definition of

core critical infrastructure set, and the public-private partnerships moving.

So, within DHS we have been busy not only maintaining -- sustaining the capacities we have, but building on those. And, by the way, I must say that's somewhat of an interesting challenge when you don't have a budget and when there's sequester. All I will say about that is if you look at the President's budget requests for DHS over the last four years, you look at what Congress has actually appropriated, including in the most recent FY13 budget, you will see that in the cyber arena we have had dramatic increases in funding. Why is that? Because I think there is a general recognition that we have to build civilian capacity where cybersecurity is involved. And to do that -- if you look around the government, where is the natural home for this? It will be within the Department of Homeland Security. That's where the core information-sharing should come, where core critical infrastructure is concerned. That is where threat information should be shared. That is where we should be talking about how to do the most we can, the best we can, to prevent successful attacks while also dealing with resilience should an attack succeed.

I don't think we should let Congress off the hook, by the way. I do think we need legislation. We need legislation, I believe, that sets forth the privacy and civil liberties safeguards that we've adopted as policy. We need legislation to make sure real-time information sharing occurs. We need some additional law enforcement tools in the digital age. And we need -- and this is peculiar to DHS but very, very important, we need the same kind of hiring authorities that are held in the Department of Defense where cyber is concerned that allow us not to use the normal civil service hiring and wage scales so that we are even more competitive than we are right now. We're competitive for cyber experts. Why? We're competitive because of the mission we're performing and the fact that if people want to be involved on what really is the foundational work where the nation's cybersecurity is involved from that security aspect, and that experiment that I talked about, the work is at DHS. So the mission itself is a huge recruitment advantage for us, but let me now say that we all understand that there are other issues that people need to take into account, including how much

they can get paid. So we want some relief there. That has to be done by statute.

And let me just close by saying you're meeting at a critical time. You've seen our people in and out all day. They're in and out all day because they're busy working on all the deliverables I just discussed. We are moving very quickly on these timelines. We cannot succeed, and this experiment will not succeed, unless there is total buy-in by the nation's operators and owners of critical infrastructure. This is the grand experiment. We intend to succeed. I hope you do, as well. Thank you very much.

[applause]

Tom Gjelten:
Hello, everyone. I'm Tom Gjelten from NPR. And I'm assuming that Congresswoman Harman will be back after she says goodbye to Secretary Napolitano. Some very provocative thoughts there from Secretary Napolitano that we're going to have a chance to respond to. Let me first of all say on behalf of NPR how appreciative we are to Jane Harman and to the Wilson Center for sponsoring this series of programs, which we call a National Conversation. And it's a great honor for me, in particular, personally to be able to moderate these discussion.

Now, it was interesting to me that Secretary Napolitano talked about what she called there in the end a grand experiment. She said this is the first time -- talking about the cybersecurity challenge, this is the first time that the United States has really, in a sense, depended on the private sector for such an important partnership role. You know, I noticed that one word we did not hear at all in Secretary Napolitano's comments was the word “mandate” or “mandatory,” and what a difference that is from a year ago in the time of the Collins-Lieberman legislation, when mandatory approaches were very much a part of the discussion. And now the word that she used and said instead is “incentive.”

But I also noticed that she didn't seem 100 percent convinced that this approach was going to work. She referred to it as an experiment. She said that she wasn't completely convinced that the private sector is ready to fulfill its mission. So I'd like to begin with that point. I mean, I think this is a really provocative idea that a

security problem of the scope and scale that we're facing in the cyber domain, the government is really depending on the private sector to play a huge role, and it seems like the verdict is out on whether this experiment is going to be successful or not. So I'd just like to go down the line here and get your own thoughts on that and whatever else caught your attention in the Secretary's speech. First, Secretary Chertoff.

Michael Chertoff:
Right. I think that it is kind of a novelty. I mean, we're used to the idea that our security, our national defense, our law enforcement is largely a public responsibility. I mean, we may have private guards, but we don't really expect the private sector to defend itself against attacks for the most part. Obviously what's different here is you are dealing with assets and people that are largely distributed throughout the United States in networks in private hands. So for the U.S. government to own a major responsibility for defending these networks would put the government into everybody's computers and into everybody's networks, which I think we don't want to do as a people. So that means the private sector has to shoulder the major responsibility. But here's where I think the Secretary's right in saying it's a two-way street. You've got to step up and take that responsibility. If people in the private sector said, you know, "I operate critical infrastructure but I don't want to invest in security because I don't really care whether I go out of business or offline for a couple of days." That's not an acceptable answer. because as we saw in hurricane Sandy and we saw in prior hurricanes, a lot of people depend on that critical infrastructure. So there has to be an acceptance on the part of the private sector of their obligation to protect those assets and their employees. And it's got to be a collaborative effort.

I think that the private sector has indicated it wants to do that, and assuming we can put mechanisms in place -- which we can talk about, you know, in a little while -- I think it can be done. But I do think her message is, at the end of the day, if it's not done and if the private sector doesn't step up, and particularly if there then is a major event that causes significant loss of life or damage, the public will demand mandates and they may not be the mandates that are the most intelligent or the most sensitive in terms of the private sector.

Tom Gjelten:
Ambassador Taylor, you've worn both hats here. You've worn both security hats, in the government and now in the private sector.

Francis Taylor:
You know, I find the private sector really does understand its responsibilities here, and the difference may be in scale, you know, the amount of money that's required to be invested, and I think that's always a discussion, but the idea that the private sector does not understand from either a reputational, from a risk, from a customer value perspective the importance of this, I think we've gotten to that point very clearly now. The question for partnership is how does that partnership work? And there are many definitions of partnership. One is top-down, one is bottom-up, but I believe that the partnership has to be a partnership of mutual responsibility and respect for what we each bring to the table.

Tom Gjelten:
Steve Flynn.

Stephen Flynn:
Yeah, I guess I would say a little bit -- there's an element of this that his novel in that probably, if we use the Cold War as our stepping off point -- but I think a lot of this is "Back to the Future." If you really look at the nation's response to the Second World War, it wasn't basically saying public sector, you know, kindly take care of this problem for us. We mobilized the private sector, we mobilized the civilian population, we mobilized the academic community because the threat required an all-of-society response.

I think, for me, just as a stepping off point about this threat, this particular issue is so sobering. You know, back to the issue of looking at the al-Qaeda threat in the late 90s, there was some debate in the national security circles about whether this really was the serious threat. And while I fell down pretty hard that it was, I could, you know, accept that there was some disagreement. For this particular threat, I know of no other -- else where there is such consensus amongst the top officials who look at it, as well as everybody who's an expert on the private or public side or academic side, that it is a real problem.

And yet we're barely getting our act together on how to deal with it.

So I think the threat warrants the kind of mobilization effort that is required that we haven't seen in the past, beyond just saying, "Hey, government, can you sort this out? We want to do our kind of pursuit of happiness on the side here. Thanks very much." But there's a huge choreography challenge. It would just add one more wrinkle. You know, part of the reason why we need private sector engagement is because these networks are global. Or if we take infrastructure. A lot of the juice, the power we get up in northern New England area comes from Quebec. So if you just have a purely domestic conversation amongst state, local, and tribal players for networks that sprawl across borders, we're not going to get there from here. Yet private players are already in those markets because the systems work that way and so that's another reason why the partnership is so critical.

Tom Gjelten:
Well, Steve, you mention World War II and the role of the private sector, which is interesting. I heard Franklin Toya [spelled phonetically] of the National Counterintelligence executive make the point that in World War II, the private sector, albeit it played an important role, it was very much a support role. It was very much in the rear guard. If there were to be a major cyber confrontation, cyber conflict, the private sector would not be in the rear. The private sector would be on the frontlines, and that's a very different situation, isn't it, Secretary Chertoff?

Michael Chertoff:
I think that's exactly what the difference is. It's not just a question of providing the material and the support, but in this case the actual conflict, so to speak, would be in the private network. The Secretary mentioned the Saudi Aramco case, which is public, in which there was a destructive attack on the computer infrastructure of Saudi Aramco. So there you have the tip of the spear are the people who are actually operating in the network. This requires actually, if we think very carefully about how we plan, for a coordinated response. If there were a cyber 9/11, obviously you'd want to have the private sector and the government working together. To do that, you've got to have a lot of planning in advance, you've got to have a

mutual understanding of what's operating on the network, both what's coming in and what's within the network. And, again, that's a little bit new for us. It's going to make some people uncomfortable. Although I used to say to people when I was secretary, "Accept the fact the government is going to have be involved in your network. The question is which government? The U.S. government or the Chinese government?" But you're going to have a government. So there's no way to say we're going to somehow take cyberspace and remove it from the domain of conflict and threat.

Tom Gjelten:
You know, I promised Jane that I would not quote anyone from lunch, but I think I can say generally that there were a lot of concern about the economics of cybersecurity, because in order to protect the networks to the degree that we I think all agree is necessary, it's going to require some real expenditures, a big investment. And that whether the private industry is able to come up with that kind of funding I think is a question, whether the government can come up with that kind of funding right now is a very big question, whether the government can require private industry to spend that money is a big question. Does this mean that the risk is just something that we have to accept? Ambassador Taylor.

Francis Taylor:
I think risk is a part of the world we live in. There is risk in the physical space, there's risk in the cyberspace. The question is what's your strategy for mitigating that risk and are you going to, you know, fire a howitzer at a gnat or are you going to take the very specific steps to deal with the risk at the right level to ensure you've mitigated it appropriately? So -- and this is expensive, but it's not, you know, so expensive you can't do it. There was a discussion we had earlier that said 80 percent of the things that can thwart many of the risks that we face are simple patching and vulnerabilities that we already know about. So, you know, it's not that it's so expensive, it's getting people to do it and to do it in a consistent way.

Tom Gjelten:
But those -- I think that the reference there is not to the threat of a massive attack on infrastructure but rather smaller-scale attacks. What about -- how do you protect

against, you know, the cyber 9/11? That's a threat of a whole different order, isn't it, Steve?

Stephen Flynn:
Right. You know, I mean, the qualitative change that I think we're all coming to grips with here relatively recently is we're moving from the cyber threat being essentially stealing data or disrupting networks to basically commandeering those networks, and then therefore there's a risk of sabotage as a result. You know, you don't need to mobilize a team and get on an airplane to cause destruction to these systems. You can potentially do it, as it was laid out by Jane Harman at the start, whether it was generation sub-station or pipeline or hydroelectric dam, we can go on, these systems are increasingly on the net. Not all of them. In fact, one good-news story is some of them are so old and really broken that you can't actually commandeer them in these ways. You'd have do it in the old physical world, but we're going to move them into that realm.

Stepping on the economics. I mean, an element of the challenge here is we're coming late to the game and we're kind of boiler plate on security safeguards or systems that were not built to be, essentially, made safe, certainly for the threat we have. So it's a bit like taking a raised ranch home and trying to make it handicapped accessible. Okay, it's going to be expensive, ugly, and not work well. And everybody's looking at this legacy infrastructure we have right now and going, "Oh, my God, it looks like trying to do that." What we really need to do is talk about designing into the systems, the safeguards. And that's not a conversation we -- that we have really started. And that's part of where I am in the world of academia. I mean, Silicon Valley works and Kendall Square up in my neighborhood works because it's directly -- private sector is working hand-in-glove essentially with the folks who are developing the ideas and the applications. But that security conversation's almost always happening after those things are developed. We have to figure out how we design this in. The economic case is clearly simple and it's overall if you want -- if a business wants to continue to provide its service, it probably doesn't want to be disrupted. The cyber threat is going to disrupt it. Right? How in a cost-effective way do you ensure the continuity of that business? That's what we need to have as a conversation.

Tom Gjelten:
Secretary Chertoff, that was -- Secretary Napolitano referred to the failure of the legislative effort last year, and I think a lot of people who have been working at this effort were really disappointed that that huge effort ended in failure. How do you see the political environment now different from that? Have there been lessons learned from that?

Michael Chertoff:
I mean, I don't know that I would say it failed as much as it ran out of time. I was involved in it. I kind of helped out pro bono with some of the members in the Senate. I think that they were migrating to a compromise. It was a pretty broad compromise and then the session ended. There are challenges both on the information-sharing side and on the standard-setting side. And there were, you know, legitimate criticisms or concerns that were raised. On the other hand, we often live in a world in which, you know, the enemy of the good is the perfect, and you're not going to get a perfect bill. So I do think there's an opportunity here. What is important is understanding the urgency, and I think that was the initial point that the Secretary made, that maybe there's not a real appreciation -- this is not a theoretical discussion, but that we're actually dealing with a threat not only that's happening in the area of theft in intellectual property, but that we're beginning to see disruptive behavior like Saudi Aramco. And I can tell, you having lived through 9/11, been in -- you know, in a position of responsibility since then, if, God forbid, we had something like that in cyber, you would see legislation, and the people who didn't like what was coming last year would be really unhappy with what you see. So the time to think about this and plan is in advance, not in the immediate aftermath of a big event.

Tom Gjelten:
Ambassador Taylor, I remember from covering this in debate last year, there were a number of comments made by people on one side that owners of critical infrastructure, and particularly in the utilities area, too often downplayed the threat. Now, Secretary Chertoff just mentioned that there's more sensitivity perhaps now to the urgency. Would you agree with that?

Francis Taylor:

I think we all have come to understand the nature of this threat and how it impacts our business models, how it impacts our ability to do research, protect our intellectual property, and those sorts of things. I wouldn't say people downplay it, but it's the -- at what level of risk are we going to be held accountable for managing to it is maybe a question that some would ask. But understanding the risk and the threat to operations and our people I think is very clear in the private sector.

Michael Chertoff:
You know, Tom, let me say one thing. I think one challenge there's been for the private sector is that this whole process becomes very mystified. There's a lot of jargon and engineering discussion, and I know from being on boards and dealing with boards that there are a lot of folks like the utilities folks who do actually invest in and focus on it. There are a lot of civilians who hear this jargon and they throw their hands up and they feel it's so complicated, either we can't deal with it or we're going to make it a tactical problem. In fact, it is not too complicated. Frank's exactly right. You want to manage the risk, but if you can understand it and you can translate it into plain English, there are things you can do. But you have to make decisions. Do you allow everybody to bring their own device to work and simply move data back and forth freely? Does everybody get to take their own thumb drive and stick it into the network and then bring God knows what into the network? So these are not technical issues, they are policy and governance issues.

Tom Gjelten:
But isn't it true that private entities that cut corners may benefit sort of in the short run, you know, by not taking those measures?

Stephen Flynn:
Yeah. I guess I would come to that, is that this is where we're kind of misdirecting. We do need standards, right? If you are a large company and you are doing the right thing and some of these [unintelligible] cost, then a smaller player can basically say, “Well, I'm not going to do that. I can offer a different, obviously, price point.”

Tom Gjelten:
Right.

Stephen Flynn:
If a standard is set and people can have some confidence that they're enforced, then we basically have a level playing field. The real issue, though, is lack of trust between many private players and the public, say, about where we're going to -- whether the standards will make sense, whether they will be -- they won't actually address the problem. And so the real conversation should be about that. What is it -- how do we confidently get the two-way street in developing the standards, versus that the standards are somehow something we can live without? There are mechanisms clearly that do this with third parties, insurance, and other things. They don't have to be purely governmental, but we've got to stop pretending this is all just happiness and best practices. I mean, we've been doing this for how many years? The threat is only growing and we are faced with the reality we're not making much progress. So that would suggest the best practice to-date is a lousy practice.

Tom Gjelten:
Well, Frank, you're up here representing the private sector, so -- Steve used the S word, "standards."

Francis Taylor:
I'm Frank Taylor, I work at GE

[laughter]

Look, standards I think are important, but they have to be realistic. And, as Mike said, often this conversation is so threat-mongering that people get turned off. So I think --

Tom Gjelten:
What do you mean by that?

Francis Taylor:
Well, you know, you -- "the world's going to come to the end tomorrow if you don't do this." Well, it's not that dire or drastic. And so I think a rational conversation about realistic standards that address the vulnerabilities is what needs to be had. And a lot of times when the conversation is around, "Well, you shouldn't do business and so-and-so." Well, you know, companies go where revenues are generated. Where there are customers, they're

going to sell things. So having a rational discussion about what those standards should be to address the risk, I think most companies would come to the table and have that discussion. But it can't be out of threat-mongering, as I call it.

Tom Gjelten:
Have you been guilty of threat-mongering?

Michael Chertoff:
No, and I don't think that I'm mongering the threat here. I just think you just have to open the newspaper, and that's only what's publicly reported. I mean, the things I know that are not publicly report are obviously also, you know, important knowledge, too. And that's one of the reasons I think, by the way, making classified information either available because you declassify it or because you allow to people to be cleared is a very important part of this.

But, look, I mean, I think in terms of standards, what was -- what's interesting about the process proposed now with voluntary standards is it would be collaborative. It would involve the private sector and the public sector. Setting kind of general performance-based standards. That requires the private sector, as well, to recognize that they are hurt if there are outliers that don't ring up their capabilities to a reasonable amount of risk management. And I think that's where the experiment is, if they do recognize that we may get some good standards going forward.

I do think that it's got to be dynamic. This is not a static threat. And it's got to be a recognition, as was said earlier. There's not risk elimination, there is risk management. But the one tool the government does have, which that I think is important, is looking at the liability system, and I think the insurance industry can play a role here, and using that as an incentive so enterprises understand that if they do make an investment to a reasonable degree and they do meet these standards, that they will get some measure protection, which is exactly what you need to spur investment.

Stephen Flynn:
If I could add, I just want to -- I think it's so important in this backdrop and is why this conversation and the

Wilson Center hosting it other places is so important. We can't have this conversation without bringing the public IQ up a bit. In part, again, that hygiene issue is largely our behaviors, okay, at the end of the day, and so this is really something at the student level and at the household level. It's a real act of leadership to get this out of just purely talking to -- even after I talked to Steve Sweet [spelled phonetically] in government. Because that's not -- that's going to keep the backdrop for the public to say, "I'm willing to pay or support one way or another." And if we don't get there we will run into a problem.

An instance of this is the utilities. Okay, most utilities can't just set the rates, they are governed by states. And those utility boards overseeing it are trying to keep the costs for its users down. If you are a utility, you're worried about trees that are colliding with their lines, as we know here in this area and up in my area in New England. You're worried about aging equipment and backup sub-stations. Those all have risk to disrupt your service. So the government comes in and says, "You need to take on this new set of problems with these new costs, but, by the way, there's no relief on your price because the public doesn't get the rates may have to go up. We have a problem." They make users both public, but also have the companies that depend on that have to be a part of the conversation to say, "This is an acceptable cost I'm willing to bear because it will provide me a service that I need." And anybody who lived up in the Northeast -- it wasn't just New Jersey and New York. I was in Connecticut. Three-quarters of our state was out of power. I thought -- I used to think I was in a first-world country, but now I discover increasingly that that's a questionable proposition. The reality is you need that to have a civilized country, and I think most people after seven days without power would be happy to pay a little bit more on their rates. But we have to understand where these are connected.

Tom Gjelten:
Well, I know, because I was at this lunch today, that we have an especially distinguished group of people in the audience today, so I want to make sure that you all have some opportunity to ask questions. I think we probably have microphones on both sides. And if you're willing, I think it would be helpful for you to identify yourself and your affiliation or your company first. So let's open the

floor now to questions from the audience. In the back, there, we have one.

Female Speaker:
Hi, my name is Dana Cook. I'm with the urban studies program here at the Wilson Center.

Tom Gjelten:
Okay.

Female Speaker:
I have two questions, if I may. Be patient. I read in this report where they were talking about a lack of cyber protocols, and then he went on to say that the problem is that nobody wants to take accountability for creating the protocols or governing cybersecurity. Who will be accountable? Everyone says we need these laws, we need these accountabilities, we need these protocols, but who's going to step up and take responsibility for creating them and saying, "Let's stick to it"? And my second question is, with the number of mobile devices being used to commit cybercrimes, and they're promoting -- they're helping cyber terrorists and they no longer need to sit at a stationary terminal to commit these cybercrimes, and since mobile and cloud computing is growing rapidly, it's out of control, who's going to take responsibility for that? Who's responsible for governing cloud computing and governing these mobile devices and controlling the number of people who can use them commit these crimes? Thank you.

Tom Gjelten:
Well, presumably the framework that is going be rolled out this fall as a result of the executive order is going to address some of these issues, right?

Michael Chertoff:
Some of them. But, I mean, I think you put your finger on a really important issue. First of all, nobody controls who winds up mobile devices. I mean, every enterprise can set its own requirements and standards, but in general, in the world at large, it's been close to anarchic, or maybe you just want to say libertarian. And, by the way, there are people who are absolutely committed to the idea that any regulation of the Internet or this kind of communication is problematic, and there's good reason to be very, very leery of doing that. So I think it's going to

be much more enterprise-specific and it's going to be a lot about standards.

On the issue of who will bear the responsibility if there's a catastrophic problem, I mean, that's kind of a feature of American life. There will be a round of finger-pointing, there will be another 9/11 Commission, and we'll go back over all of the things we should have done and all the reports that were written before will be brought out and people will say, "Look, we warned you." I think that we're trying really hard to avoid that by putting into place a set of practices and standards and capabilities in advance that will reduce dramatically the likelihood of that kind of catastrophic event.

Stephen Flynn:
I guess it reinforces, though, for me that there's not an easy answer, of course, in this, about how we really have to talk about this as -- in the design stage. We have to find a way in which we're having this conversation I would argue in the university world and where in the high tech world where these are being done. But not to say that's going to get the ultimate outcomes, but at least there's some sensitivity there that have to be in place. And that really has not begun. We're -- again, we're dealing with this almost after the fact, trying to develop safeguards, being aware of vulnerabilities.

Government does have a role to play in supporting accountability. We've learned this over a long time with loss of systems. Standards -- again, I think the key is, that we've talked about, that they're dynamically forged, that the owners and operators who designed the system are helping to design the standards. The enforcement ideally should be third parties, user base, and so forth here. But there's usually almost always is a need for the government to make sure for that, in fact, outliers are not outliers or that they're isolated from the system. And that's the only way we know have to do this stuff. It is -- I think we have to talk about a more robust, dynamic process of setting standards, but I think we also have to recognize that some of these issues, there does need the ability of policing, and that may not just be domestic. It's on the international scale. That has to move forward.

Tom Gjelten:
Larry.

Male Speaker:
Thank you. Larry Couton [spelled phonetically]. I'm with the Internet Security Alliance. I want to associate myself with whoever made the comment before that we're kind of in the very beginning of this discussion, because I think we get some back and forth thinking when we talk about the threat and how we're combatting this. It's my understanding -- and I'd appreciate if the panel would tell me if they think differently -- that the standards that we're talking about, which do exist, solve 80/90 percent of the problem, A, currently already exist and, B, those are going to combat the low-level threat. I don't know anybody who thinks that the standards or the framework that comes out is going to be effective against this advanced, persistent threat that's -- could take down the electric grid, et cetera, et cetera. So that's the area that I'm interested in.

Secretary Chertoff said, and I agree with him, that the private sector is going to have to step up, and I think the private sector, as Mr. Taylor said, is willing to step up. But I'm curious as to what the government does to assist the private sector, because if we're going to deal with this massive threat, we're not talking about a little more money, we're talking about a lot more money. Studies say five, eight times as much money. So we're going to need big incentives for that. What can the government do to assist the private sector in taking on this unique and fairly substantial new role?

Tom Gjelten:
Important question.

Michael Chertoff:
So, I would -- first, I think you're absolutely right, Larry, that you have to separate the majority of enterprises and small businesses that probably need to make a relatively modest investment to take care of the 80 percent to 90 percent. Much of the discussion I think we had here with the Secretary was about the top critical infrastructure, which the department's identifying. Those are enterprises that, if they fail, there's going to be a humongous effect. I mean, if, God forbid, for example, the air traffic system failed and planes start to have a -- you know, fall out of the sky. I'm not going to say that's going to happen, but that's an idea of something. There

you do need to have a focus on the advanced, persistent threats. And there are going to be different standards there. What's it going to take? Some of it is going to be incentives to get the enterprises in that critical field to raise their degree of investment, recognizing that, as a benefit for that, they should get liability protection and caps so that they don't have what happened in the World Trade Center after 9/11 where everybody sues the owner. And, believe me, that's a road to bankruptcy. So that's one set of incentives.

Second, I do think the government has to be tightly bound in terms of information-sharing and sharing of techniques and capabilities. That's going to require maybe looking at the law again and it's also going to be addressing people who don't like the idea of the government being involved in this. But if something happens really fast, you're going to want to have the government working side-by-side with the private sector to stop that. So I think those are a couple of areas we're going to have to work in.

Stephen Flynn:
If I could add on the critical infrastructure component the high-threat realm. I think one of our problems is there's a little bit of -- which I think is causing us some challenge, of cyber is now all what everybody is focusing on, and that's where the resources are going; we all should be talking about cyber. I think we need to talk about the state of our infrastructure and the range of risk confronted in infrastructure, which cyber is one of those. And as an advanced society, guess what, you need infrastructure to work if you want to stay advance. If you don't maintain it, if you don't upgrade it for the kinds of weather events and stresses of use. So I think of the element of being more successful is not purely disaggregate the cyber conversation from the larger one you have with the public about how do we assure that mobility, communications, finance, water, all this happens, because one of the real disruptive risks, the one that's clear and present now is cyber, but that's not the only risk. Because until then [unintelligible] probably not going to be willing to talking about investing in infrastructure safeguards to assure its continuity. So I think we really need to broaden this conversation away from just cyber. That's the element of cyber-physical that I think is an opportunity that we probably haven't harnessed yet.

Tom Gjelten:
Before we go on, I'd like to get Frank Taylor's response to Secretary Chertoff's suggestion that liability protection might be a very significant incentive. Is that a -- how significant an incentive do you think that would be to companies? Would that be a sufficient incentive on its own to justify them making much bigger investments than they're willing to make right now?

Francis Taylor:
Let me -- I'm not a lawyer, and therefore I can't speak for our legal department. But I think a framework of incentives that maybe limits liability and that sort of thing would probably be very, very attractive. And that takes legislation and it takes an understanding of how this fits into the overall protection of the infrastructure of the company. And so I think that would be attractive going forward.

Tom Gjelten:
Other question? Right back here. You.

Male Speaker:
Thank you. My name is Jacob Warwick [spelled phonetically]. I'm from the Center for the Study of the Presidency and Congress. I just wanted to ask what role, if any, should reforms to the Federal Energy Regulatory Commission, FERC, play in creating required standards for energy companies? I'm thinking about, for example, the GRID act.

Tom Gjelten:
You're thinking about what?

Male Speaker:
The GRID act that was in Congress a couple of years ago and failed.

Tom Gjelten:
Any of you familiar with --

Stephen Flynn:
Well, I could take, I guess, a bit of a swipe at this here. You know, again, part of the challenge is disaggregating utilities from their customers. And take the Port of Authority of New York, New Jersey. It moves on any given day actually at rush hours, which is the way it is in New

York usually. It is about 1.8 million people that are in a port authority facility. That's in the tunnels, that's in the bus terminal, that's in the airports, sea ports less, the pass system, and so forth. All that requires energy if it's going to work, as we saw, again, with Sandy. That customer is not part of the conversation with the utilities, ConAd [spelled phonetically] and so forth, to say, "What are you doing to make sure that this power stays on? Because our mission is critically dependent on your mission." And so I think one of our challenges here is to broaden the focus of not just beating up one sector to do more, but basically finding a way in which that sector is working with both -- is able to make its case and therefore ideally get the funding stream that goes with that to the public and to other critical sectors who are dependent upon them. That's where I would be nudging this process along.

Michael Chertoff:
I would say -- by the way, I think the electric sector actually does. You know, we do a lot of work with them, and they actually are quite focused on this issue and I think are looking continually to kind of upgrade. But, remember, if we go to a smart grid, every node of that network grid is going to become a potential aperture through which malware can come into something. So, again, that's what I mean about it being dynamic; you have to stay ahead of what's happening.

Tom Gjelten:
I know from talking to private sector that there's a lot of concern about a compliance mentality being the product of the kind of standards that we're talking about.

Michael Chertoff:
Yeah.

Francis Taylor:
We -- certainly regulation is helpful and it's hurtful, if it's done poorly. And so a compliance regimen in this area, in my view, is fraught with danger if it's not done properly. It doesn't mean you can't have compliance, but it has to be done in partnership with the public and private sector. Otherwise, if it's mandated without -- and we had a discussion about CFATS and how that rolled out of DHS and the challenges of --

Tom Gjelten:

This is the chemical facility --

Francis Taylor:
Chemical facility, but not a lot of private sector input to that, and it adjusted over time, but it doesn't -- just coming out with a compliance regimen without real collaboration or cooperation on this. And I would -- you know, the notion that the private sector does not understand this risk -- we operate globally. We operate with the Internet and cyber systems being critical to our business model. We're attacked every day. So we have an understanding of the impact of this. The question is how do we work with governments, and not only governments here but governments around the world, to protect what's on that network and criminal acts against that network that are occurring around the world that impact us as well as impact national security and certain regions around the world.

Tom Gjelten:
I'd like to invite any of the folks who were at lunch today, if you have any comment to make or question, because I know you have a lot of concerns that I think deserve to be represented. Yes. Dan, right?

Male Speaker:
Dan Donohue [spelled phonetically] with Caterpillar [spelled phonetically]. This is a really tactical question, but one of the things that we've seen is there's a major vulnerability caused by poorly-written code, code that underlies our applications, our operating systems, our telecommunications devices. You know, we've talked about designing security in, but having code that's stable, that's secure, that's just not happening. You talked about Silicon Valley, you talked about the -- Route 128. The same problems are inherent in all of those companies and all of those locations. They write bad code. So this is something that can't be done purely on the private sector, it can't be done purely on the government sector, but has anyone really given that a thought? And how can we change the whole vulnerability landscape that we exist in?

Michael Chertoff:
You know, I would say, first of all, worse yet. Some of the code's not being written in Silicon Valley or Route 128, it's being written on the other side of the world, and sometimes the problems are deliberate rather than accidental. You know, there's a real push to get code out

quickly and to update, and for a long time in this domain, the pressure was, you know, get new things out more quickly, and the security element was not a major feature. The customer has a lot of say here. If the customer starts to look at this and wants validation -- and it's true not just for the software, but the hardware, too -- that becomes supply chain security, which is a whole other chapter of what we need to talk about.

Stephen Flynn:
Yeah, and that's -- the acquisition rules are key, but not just government acquisition -- that could lead the way -- but obviously corporate one. If you just take the gaming industry, the gaming industry 10 years ago were like everybody in the garage, but now the gaming industry is basically three very large players who push out products for lots of people. That means there's a lot more leverage in the market to say, "Before you give me X product, I want it to have some due diligence here with regard to the code." I think not enough has been done about that conversation, clearly, and we have to look for where there is leverage points, but, again, there also is a sense of cultural change that is going to be truly challenging in this information age that, in fact, there's risk out here that we all, as citizens of the cyberspace, have to take responsibility for, just -- as opposed to just purely policing it from governmental activity.

Tom Gjelten:
You know, I'm a journalist, and one of my interests as a journalist is always to tie these discussions to current events and news, and Secretary Napolitano pointed out that the solutions that we're talking about, the approaches that we're talking about in this area are going to require a level of intimacy, was the word she used, between the public and the private sector. And I'm just curious if any of you have any thoughts about whether these recent revelations about collaboration between the NSA and tech companies have jeopardized or made more difficult or tainted the whole notion of collaboration between the private sector and the government.

Michael Chertoff:
You know, and I -- first of all, as she said, and quite rightly has to be emphasized, what we're talking about is completely different from the other program. Although experience shows in the public discussion, a lot of stuff

gets conflated. That being said, I think there's -- there is a risk that for some people, particularly when there hasn't been a bad event, they can get themselves worked up by speculating or imagining or hypothesizing how all this is going to wind up with some Big Brother type of thing. There are structural changes in our society with the availability of big data in the private sector that are not going to be rolled back. We are largely dependent on networks for not only moving information, but making things happen. Anybody who thinks that it's better to let things develop so that criminals and terrorists and adverse actors can exploit it, is going to be in for a very rude awakening. But I do think we need to be honest about it, we need to be clear, and, frankly, since you're a journalist, I can say it behooves the media to spend time actually explaining with clarity what is being proposed, as opposed to simply taking what one disgruntled person may spin and putting it out there as if it's the gospel.

Francis Taylor:
I agree completely. I think it colors the dialogue or the discussion. I think there has to be a public discussion about these issues for people to really understand it, and in many cases these are very complicated issues that people haven't thought about in terms of their cyber presence and how that is potentially exploitable. We hear about identity theft, we hear about theft of credit, but the more sinister aspects of this are not very clear to the public, so the revelations of the last couple of weeks have made it difficult. There was one telecom that said the government had asked for 5,000 requests in the last month. You read between the lines, you know? You don't do a law enforcement investigation in this country without going to get the cellphone records. It's all a part of how law enforcement gets to the facts, but that was all kind of in this big push about government involvement in the private sector. So explaining that a bit more efficiently in terms of what it really means and how this part of infrastructure protection is quite different from intelligence collection and those sorts of things I think will go a long way towards the American public better understanding how this must work.

Stephen Flynn:
I think it reflects in part a transition that our government is going through, that this conversation and the Secretary's remarks helped to highlight. You know, we

really took the position right after 9/11 that the security of dealing with the terrorism threat was largely inherently governmental. The job of all of us, the citizens with the shop and travel, we're going to put our national security apparatus on steroids and we're going to make this threat go away. This many years later, we realize the threat has not gone away, it's more, and also that the only way we get at this threat, because it's targeting the civil sector, is to engage private sector and broader civil society. Yet our Cold War apparatus is still sort of ticking away at this is inherently governmental, it's a patriarchal [spelled phonetically] sort of closed system. There are some things that clearly have to be closed, but I think what the government's starting to realize is that it needs to probably err on the side of more openness about what it's doing. I mean, the President certainly is saying that we need to push out a little bit more what these systems are, but the days we can work behind closed doors and sort of just take care of problems are gone. And if this messy situation we have right now helps us make that cultural shift that much quicker, I think it will be a positive outcome instead of a negative one.

Tom Gjelten:
Well we've covered a lot of territory here, but I want to give you -- before we close, I just want to give each of you an opportunity if there's some point that you've left unmade or some comment that you want to sort of throw out there as your final comment, parting thought.

Michael Chertoff:
No, I just want to thank Jane Harman, I want to thank the Woodrow Wilson Center for highlighting this. I think we are at a time when people are focused on this. I think it is a little bit of a novelty to talk about the private sector actually having responsibility and accountability, at least at the critical infrastructure level, so we need to continue this discussion, but I would say let's not continue it indefinitely. Action has to follow, or we're going to be in an unhappy place.

Francis Taylor:
I would echo Mike's comments, and the private sector really does understand this risk. It's a risk to our reputation, it's a risk to our customers, and we worry about that every day. So it's not we're sitting with our heads in the sand, thinking that the government's going to tell us what to do.

This is real, day-to-day work that we are doing. The integration of that within the critical infrastructure structures of this country and other countries who are asking the same questions will be the real challenge, and that's where the partnership has to be, that's where the dialogue has to be. I'm reminded -- I spent 30 years in the Air Force, and 20 years ago the military was having this very discussion about who's in charge and who's going to be accountable, and we solved that in DOD some years ago. And I see us at the same juncture in public-private discussions in terms of what's the shared responsibility, who's going to lead the way, and what are the processes that we're going to use to do that?

Tom Gjelten:
Well, from a political science point of view, it's a pretty fascinating moment, isn't it?

Stephen Flynn:
No, absolutely, and I guess some final -- Frank and I were talking a little bit at the outset. The challenge of a panel like this, saying we're representing sectors, you know, and obviously these sectors are so diverse, but I'm delighted to have this chance to be a part of this conversation. Private-public, I would argue, academia needs to be a part of this, as well, the reason we went on, and I guess there's a theme to leave, is this need to design into, and that means -- the Manhattan Project, which I mentioned earlier, was taking a bunch of people who were very smart who knew nothing about national security and harvesting that expertise to deal with a threat. We have that. That's the greatest strength, I think, of this country as we know right now. People still knock on our door to come here, yet we really left academia largely on the sidelines from this conversation, so it's partly private-public [unintelligible] I would argue academic, as well.

Tom Gjelten:
Private-public-academic. Okay. All right, well, Jane Harman, thank you so much. This has been I think, from my point of view, a really useful and interesting discussion, and I'd like to thank the Woodrow Wilson Center and my own organization, NPR, for sponsoring this.

[applause]

[end of transcript]