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,

Pr

WWC:

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 cm Beg0 0 0yeesT Q q0Tc 50 0 0 50 0 0 Tm /T 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.

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, 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

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 id

WWC

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 --

I think we all have come to understand the nature of this threat and how it impac

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
Tf75and0.24 0 ave to be

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

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

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

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 ac

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

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]