



Center for a
New American
Security

DEVELOPING A NATIONAL CYBERSECURITY STRATEGY

INTRODUCTION BY:

**DR. KRISTIN LORD, VICE PRESIDENT AND DIRECTOR OF
STUDIES, CENTER FOR A NEW AMERICAN SECURITY**

MODERATOR:

HARRY WINGO, POLICY COUNSEL, GOOGLE

FEATURED SPEAKERS:

**ELLEN DONESKI, CHIEF OF STAFF, U.S. SENATE COMMITTEE
ON COMMERCE, SCIENCE, & TRANSPORTATION**

**LIESYL FRANZ, VICE PRESIDENT FOR INFORMATION
SECURITY AND GLOBAL PUBLIC POLICY, TECHAMERICA**

**RICHARD HALE, CHIEF INFORMATION ASSURANCE
EXECUTIVE, DEFENSE INFORMATION SYSTEMS AGENCY**

**CHRISTOPHER PAINTER, DIRECTOR OF CYBERSECURITY,
NATIONAL SECURITY COUNCIL**

**PHILIP REITINGER, DEPUTY UNDERSECRETARY OF NATIONAL
PROTECTION & PROGRAMS DIRECTORATE, U.S. DEPARTMENT
OF HOMELAND SECURITY**

**12:30 PM – 2:00 PM
THURSDAY, SEPTEMBER 18, 2008**

**TRANSCRIPT PROVIDED BY
DC TRANSCRIPTION – WWW.DCTMR.COM**

MS. KRISTIN LORD: Good morning, everyone. Thank you so much for joining us today. I'm Kristin Lord from the Center for a New American Security. It's my great pleasure to welcome you here today to this discussion of America's cybersecurity and what steps the United States should and perhaps even should not take to protect it.

We're very pleased to be teaming up with Google and appreciate them hosting us here. Combining Google's cutting edge expertise in information technology with our own pragmatic and multidisciplinary approach to examining the national security threats that our country is facing today and also is likely to face in the future. Our two organizations, Google and CNAS, chose to co-host this particular event for two reasons.

First, we think it's very important to understand more fully the scope, severity, and complexity of cyber threats to U.S. national security, the choices our society must make in order to confront those threats in a judicious fashion, and the specific steps we must take to build and implement a national security cybersecurity strategy.

Information and communication networks, as I think we all know, are now central to U.S. and global economy, national defense, and indeed, our every day life. Our government clearly recognizes this fact and has upgraded cybersecurity as a national priority. The White House recently published a cyber policy review and the Pentagon is establishing a new cyber command.

And I personally have been struck by, in conversations with our most senior military leaders, how high they place cybersecurity on their lists of priority even at a time when are serious and in many ways, more familiar threats like Afghanistan and Iraq are very much on their radar screens.

And second, both Google and CNAS recognize that any successful effort to understand and cope with this threat, and threats of cybersecurity, will require the active participation of both the U.S. government and the private sector, each contributing their own distinctive expertise and their own distinct resources.

And this threat, in some ways, is like so many other threats our country will face in the coming years and decades. We have to recognize that no one actor, not a superpower, like the United States, not even Google, can confront the challenge of cybersecurity alone. And this is a complex and diffuse and multifaceted challenge, and it demands a nuanced and multifaceted response by a network of both American and global actors from the private, public, and nonprofit sectors.

The threats posed by cyber attacks crosses spectrum. They include a non-expert like me sees as being the most likely threats. Small-scale criminal and intelligence gathering incidents that combine to impose substantial costs on our society over a period of time. They also include far less likely but far more severe threats: strategic attacks against the U.S. financial system, air traffic control system, and electrical grids that would damage the very foundations of our economy.

And before I begin though, I'd like to very quickly introduce this extraordinary panel that's joined us today. Their illustrious backgrounds can be found in further detail on our website. That's www.cnas.org. But let me just introduce them quite briefly.

Joining us today is Ellen Doneski, chief of staff of the U.S. Senate Committee on commerce, science and transportation.

We have Richard Hale who is chief information assurance executive for the Defense Information Systems Agency.

We have Liesyl Franz, vice president for information security and global public policy at Tech America. She's also secretary of the National Infrastructure Protection Plans Coordinating Council.

Philip Reitingger, director of the National Cybersecurity Center; he's also deputy under secretary of the National Protection and programs directorate at the U.S. Department of Homeland Security.

And Christopher Painter, the director of cybersecurity at the National Security Council, and he was also a member of the team that wrote the national 60-day cyberspace review.

And then our co-host and moderator today, Harry Wingo is policy counsel on Google's Washington office here and he leads the company's work on smart energy, cybersecurity, and a range of other Internet policy issues.

And this esteemed panel is going to proceed with the discussion but I'd like to raise just a few small questions that I hope they will begin to address.

First, how serious are cyber threats? What sorts of cyber threats does the United States face right now, today? And what sorts of cyber threats is the United States likely to face in the future?

Second, in a period of highly constrained resources, how should the U.S. balance a need to prepare for both the most likely and the most catastrophic threats with other national security needs and other national needs generally?

How should our country balance the need to protect openness, privacy, and economic vitality on the one hand and security on the other?

Does the United States have a secure and reliable access to the critical minerals and materials that make up our information networks and also our hardware? And here I have to give a shout out to a brand new CNAS program on natural security that's working on these issues.

And how and to what extent should the United States engage with international patterns in protecting cybersecurity, but, especially, how should we be engaging with partners that don't share our views about censorship, privacy, and oversight?

How should the United States respond to cyber attacks, whether from individuals, whether from transnational, criminal or terrorist networks, or foreign governments?

And for an organization like CNAS, we're very concerned with at what point should the United States respond to cyber attacks with force? Under what conditions would the United States ever use cyber attacks offensively? These are complicated questions. I have no doubt that our panel will help to address them to day.

And Harry, I turn the floor over to you. Thank you very much.

MR. HARRY WINGO: Thank you, Kristin. (Applause.) Thank again, Kristin. Thank each of you for coming out, for your time and for your interest. I'm Harry Wingo. I'm a policy counsel here in the D.C. office for Google. I focus on cybersecurity issues, energy issues, and a couple of other things. We're so excited to be hosting this distinguished panel today.

This is part of a series we call Google Talks. We have these in our offices around the world, and our Google D.C. talks are something that we do every now and then to invite the community and also just experts in a particular area where there are pressing matters and this is one of the most important things that we have going on right now, cybersecurity. And so we hold these talks and we're happy to have each of you here to participate as well.

I'll be moderating the session and I'm going to ask – we're just going to jump right into questions, but I'm also going to have the panelists ask questions of each other as well. So feel free to do that as we go along. There are microphones in the aisles, so as the hour approaches, we're going to actually open it up for questions from the audience, and we're also going to have Google moderator questions that we're going to take at some point. And you can check that out at our moderator page which is <http://bit.ly/0612dctalk>.

So, with that, we're just going to jump into our questions. As Kristin mentioned the 60-day review was finished recently and Melissa Hathaway did a great job of just getting a bunch of stakeholders across the country involved. Each of you were involved with that effort, so thank you for your work on that important effort. And broad input was received from all sectors: government, military, business, and the public sector.

And I'd like to really just start off with whoever wants to jump in. What are your impressions about the 60-day review, and particularly, what do you think was the most important thing to come out of that or the most important point that was made? Whoever wants to start?

MR. CHRISTOPHER PAINTER: Well, I guess being part of the 60-day review team, I should start that. I think –

MR. WINGO: Oh, and Chris also, if I would ask, for the first round of questions, maybe if you could again say, introduce yourselves, I'm Chris Painter and after that everyone will know who people are.

MR. PAINTER: I'm Chris Painter. I was part of the 60-day review team. Before that, I was at the Department of Justice and have been involved in, mostly, cyber crime issues since 1991, so I've had a long history in that.

I think, partly, that helps set up what I'm going to say here because one thing I thought was incredibly significant, and this was – the fact that president of the United States gave a speech about cybersecurity really, really was a significant ground – just game changing move. And the fact that he gave that speech, a public speech, not only signaled to the U.S., but around the world, how important this issue was. And that's really different than any other time in our history.

And I'd like to just quote one part of that speech where he said: "From now on, our digital infrastructure, the networks and computers we depend on everyday will be treated as they should be, a strategic national asset. Protecting this infrastructure will be a national security priority. We will ensure these networks are secure, trustworthy, and resilient. We will deter, prevent, detect, and defend against attacks and recover quickly from any disruptions and damages."

That is a real incredible statement for an U.S. president to make and I think it really makes a difference, not just to the community who's been playing in this area for many, many years, but to the public and to a lot of our international partners. So I think that it is a really significant accomplishment of the 60-day study.

You mentioned that there was a lot of outreach in different communities, and I think that's another significant thing in the study. There was outreach to all the different private sector communities. There was outreach to the privacy and civil liberties community, which we talked to pretty robustly during that time, to the public, and to almost every other group you can think of. We had 40 meetings in the space of that 60-day period and got submissions from over 100 different groups that are published on the whitehouse.gov website.

As far as what comes out of the report, I'd be interested in other people's perspectives on that as well, but I think one of the things that's very important about the report is it tees up a short-term action plan, a 10-point short-term action plan, which is really not just talking about what the problem is and what the threats are, but taking it to the next level and actually start to influence some solutions. And things that are incredibly important like coming up with an incident response plan both with government and industry to actually deal with some of these attacks when they happen or other kinds of cyber intrusions. We're partnering with our international colleagues to deal with some of the issues and we'll talk more about that.

So there are a lot of key things that come out of that, and the public awareness campaign, education, a lot of foundational elements. It creates a lot of work for the government. There are a lot of things we have to do. There's a lot of coordination we have to have in achieving it. That level of coordination and working together both within government – and that's not always been true – and with the government in the private sector – which also has not always been true – I think it's a real significant step.

MR. WINGO: Thanks, Chris. Anyone else? Phil.

MR. PHILIP REITINGER: I'll just sort of emphasize what Chris said at the start. I agree completely with what he said. There's a lot of good – pardon?

MR. WINGO: I'm sorry. You're good.

MR. REITINGER: There's a lot of good stuff in the 60-day review, of course, but by far, the most important part of it was executive attention. That the 60-day review made clear that the status quo is not sufficient, that we have to treat cybersecurity as a national and homeland security problem, and that the president was putting his personal focus on this, and personal attention on this, so much so that he gave a speech to the entire country about cybersecurity and that the White House was going to lead. This was going to be a matter of focus for him. That is game changing. And in my experience, nothing is more important at driving change in an organization or an economy as executive attention.

MR. WINGO: Liesyl, please.

MS. LIESYL FRANZ: Liesyl Franz with TechAmerica. I think from industry's perspective, there are a couple of things I'd just like to add because I do agree with everything that Chris and Phil have mentioned this morning with regard to the senior level, at the highest levels of government attention to this, the coordination and galvanization that that 60-day process engendered.

But the other piece of it, I think, that was important and in a way, unprecedented was that it was a very public process and a very transparent process which really was for the first time when we're dealing with cybersecurity both from a national security and an economic security standpoint. I think that's a very important piece. The president emphasized it in his speech. Melissa and her team incorporated into the process the whole time that need to access the synergies between national security and economic growth and economic security.

So it's – rather than you use the word balance, economic security and economic growth, we use the word “synergy” between the two, and I think that really came out in the report as well, not only in the written word, but in the apparent discussions and input that the team got both from the government and from outside stakeholders. So I think that's a very important piece to keep in mind.

MR. WINGO: Thank you. Ellen?

MS. ELLEN DONESKI: Ellen Doneski with the Senate Commerce Committee. I think I'd just add that it's important that the president made this speech and has a focus and appreciation for the magnitude of the problem at the very beginning of his presidency, that he's dealing with it through a comprehensive review, that he's asked others to work with him both in the private sector.

I agree absolutely with Liesyl that Senator Rockefeller thinks that we need to engage the private sector and work in a public-private partnership to a much greater degree than we ever have in the past, so that we have an opportunity to build on the work of the report and for the president. Hopefully to a point of very senior level adviser, we would

recommend Senator Rockefeller and Senator Snowe a legislation that would recommend would be a direct report to the president's cyber advisor that would manage this issue from the White House down through the agencies and coordinate with the private sector.

MR. WINGO: Thank you. Richard.

MR. RICHARD HALE: I don't have a lot to add. DOD has been worrying about the fragility of the information infrastructure for a long time. We talk to a lot of people about what to do about that and I think maybe the most important observation from all this conversation with industry is once the CEO cares about it, it starts to get cleaned up. So the point that the CEO of the United States cares about this now is fundamental and really is a game changer.

The other point is we've had lots of studies about things. They have tended not to result in specific action plans. This one is going to. This one has already got specific actions. We can debate what the details of those are. We need to debate those, but the fact that we're reducing this to doing something about it is also fundamental.

So I think actually one of the big challenges now is going to be – trying to figure out a way to measure progress. Are we getting at the root of the problem? Is this infrastructure getting less fragile? Are we getting better at interacting with each other to deal with cyber attacks because it's got to be a very collaborative process?

So measurement, I think, is going to be one of the tricks. And again, in DOD, we've been struggling with figuring out how to do this measurement. Congress has helped us with this by demanding that we do some of this measurement and that's actually been very useful, so we're starting to make a little progress there, and we have some ideas there but I think there's a lot of work to be done.

And if we're going to throw money at a plan, are we actually getting more resilient infrastructure out of it? Are we getting better incident response, collaborative incident response? Do we have ways of helping our allies if they're attacked, for instance, cyber attacked? So measurement is going to be important going forward.

MR. WINGO: So thanks, Richard. You're absolutely right about it. If you can't measure a problem, you can't manage it. I'd like to ask the panel now – Chris mentioned next steps and there's an action plan. But as we go forward, I'd like to hear your opinion on what's next, what are some of the challenges we face, and how those – moving through those next steps be informed by some of the efforts in this area that have happened in the past. So maybe if we could throw a little history on this for people so whoever wants to jump in on that point? Phil.

MR. REITINGER: Chris started the last one so I'll do this one. Obviously, the action plan for the midterm is the action plan that's identified in the 60-day review. And lots of different players in the private sector and the public sector are going to have to participate in that. I'll tell you what some of my priorities at DHS are and they flow substantially from the 60-day review.

One of them is capabilities building. There are a lot of things we need to get done, a lot of places where DHS is called upon to step up its level of capability and so my top priority is continuing to build capability within the Department of Homeland Security.

And some of that's technology but a lot of it is people. We've got some excellent people on board but I don't have enough of them yet. I've got a lot of vacancies. We're doing a lot of hiring. Please go to USAJOBS. There are a lot of things out there. If you have cybersecurity expertise, there are slots available and we are hiring.

And I'm bringing on – we're bringing on the right leadership team. I can tell you on Monday of this coming week, the new assistant secretary for cybersecurity and communications, Greg Schaffer is joining, and he was formerly the chief risk management officer of Alltel, and Bruce McConnell, who a number of you in the audience have worked with, is going to come back. He's an alumnus of OMB and he's going to be my counselor. So we will have assembled the leadership team along with bringing in all the other people that we want to add to the current crop of great people, like Admiral Mike Brown, that we have on board already.

The other priorities, you'll recognize coming from the 60-day review. We really need to get the public-private partnership piece right. We've done – there's been a lot of effort. We need to build on the good things that have happened in the past, but we need to figure out how to streamline what we've done and really focus on objectives.

One of the problems with information sharing and collaboration is we all tend get together and talk about the importance of information sharing and then go apart and three months later, we come back and have the same meeting. That's go to stop. We've actually got to build those operational collaborations mechanisms that will drive progress, apropos of all the discussion we've had.

The third area is really the incident response and recovery piece. I think we've recognized for a long time that while we've got incident response and recovery plans, if things really got ugly, we don't have a clear enough set of rules and responsibilities and ways of working together in an actionable way, so that we are sure our responses would be optimal. We've got to solve that problem – a key action item coming out of the 60-day review.

Two other things I think that we need to work on, that are at least referenced in the 60-day review, are sort of building the underlying pieces of how we can have a more secure infrastructure going forward. And I'd suggest that a couple of them, things that I particularly want to focus on, are identity management, authentication for people, processes, and devices with privacy built in from the very start.

If we want to create the mechanisms for a secure infrastructure, you've got to have optional mechanisms that are available for people to identify so they can make effective decisions about who they want to talk with, what software they want to run, what devices they want connected to their networks.

And then the last piece is really metrics. This goes back to what Richard was saying before. And the Internet is how we distribute it. Any notion that we're going to solve this

problem top down, I think, is fallacious. We need broad, distributed action, and that requires that everybody across the infrastructure be able to make effective judgments.

Authentication will help with that in terms of operational activity, but we need good metrics so that people can say, what piece of software do I want to run? What practice do I want to implement? What will work for my organization?

So until we build out that broad base of effective metrics that are tied to actual outcomes, people will make decisions about security based on religion rather than fact. And we've got to get out of that. We've got to go to more a scientific, or database driven, decision making for security.

MR. WINGO: Thank you.

MR. PAINTER: And I would endorse everything Phil said and just add a couple of things. I think one of our industry colleagues put the sort of value proposition from this public-private partnerships the best when they said, we should be focusing, not on process, but outcomes.

What are the things that we're really going to get out of this? What does the government want from these partnerships? What does the industry want? And how do we share the kind of information that will make it valuable to each of us so we have something – we have skin in the game when we come to this and we can actually do things like build an incident response plan? You can't build an incident response plan just with the government without the private sector. You can't get the kind of situational awareness of what's going on in the world without engaging the private sector in a meaningful way and without organizing the government.

So structurally, we're trying to organize the government by having this position at the White House and tying all these government agencies together, but, also, we need the private sector for that. So I think that's an important part and that's linked – information sharing, incident response, and private-sector partnerships, to me, are all sort of linked together.

The other thing I think that's emphasized in the report is the idea of having a public education campaign which involves both raising the awareness of people about security and workforce development. The bench really isn't very deep in this area. It's not very deep in the federal space. It's not very deep in the private sector space.

Public attitudes have changed but they really need to change more. When I first started doing these things back years ago, people looked at computer hackers who were taking people's identities and stealing the money as sort of novelties. They didn't care that much about it. Now, I think with a lot of identity theft and other things, people are realizing that's important, but I think more needs to be done so people think of security as part of the technological development that they are seeing make their days and lives more useful everyday. When they're using these devices, they also think about the security aspects.

Workforce development, making sure we have trained people who understand the security element, not just the innovation element, but the security. They go hand in glove.

You can't really have good innovation if you don't have a good security base because you don't want the thing to collapse later on. You want them built together. You need to build that. And I think we outlined in the reports ways to go about that, but there's a lot of work that needs to be done with DHS and other agencies to do it.

And then, another thing, I think, that's very important is this international partnership and really working, not just with our close allies, but with countries around the world to come up with issues like how you deal with norms in cyberspace, what are acceptable behaviors, some of the legal aspects in cyber crime and other areas. We have been doing this for a number of years.

Phil and I have both – and I've been doing it most recently – both chaired something called the G-8 High Tech Crime Subgroup. And we've been working on these issues, and there has been real value in the international collaboration, but it must be stronger. And I notice we have some of our international colleagues in the audience today, one from Australia, for instance, that we've been dealing with.

So we need to really – you know, I've said that there's something like 15 or 20 different international forums that deal with cyber issues. It is, to some extent, the flavor of the day. Everyone looks at this and they want to do something about it, but we've got to nationalize that. We've got to work together to get the most bang for the buck out of those forums and really advance things that are going to make the Internet safer. And there's more I can say, but I'll stop there.

One other thing: as Phil mentioned, we also have to, as we're dealing with innovation and new technologies and smart grid and all these others things that are coming online, we need to bring security in from the beginning. We need to think about those aspects. It's a lot cheaper and more effective to do it at the outset than trying to do it with an overlay down the line and again, it helps that innovation. It is the highway that lets the cars run.

MR. WINGO: Thanks, Chris. Liesyl.

MS. FRANZ: Well, I'm not sure I can follow that up with too much detail, but what I'd like to do is at least highlight three things that I think can be done or at least, begun in the near term that build upon a lot of the work that has been done to date.

The first thing – we're looking at an action plan and the strategy set forth in the review. I think, number one, we can look at how to improve the security of the federal government. We've had a Federal Incident Security Management Act and implementation of that since 2002, but it really needs some updating. Updating to be more timely and relevant, but, also, being more effective and actually making progresses in securing the agencies. So I think there is a vehicle right now to update FISMA in Senator Carper's Information and Communications Enhancement Act, and I think that is one thing we can look at really quickly and make some progress right away.

Secondly, I want to build upon the – I think any strategy development that comes out of the review should include an international strategy, to Chris' point. Again, there has

been some good work done on building partnerships, both in the cyber crime, but also in the cyber crime prevention as well as in operation and collaboration mechanisms.

But the problem is that they can only go so far without additional leadership and enablement. We've reached out. We've talked to our international counterparts, our companies, our multinational companies so they have implications of the borderless nature of cyberspace every day. So we need to find ways to enable us to talk to our international partners and actually sit down and collaborate with them. And I think there are some ways that we can remove barriers to doing that.

And the last, I'll just highlight the public-private partnership with one specific thing that we have looked for from the industry side for quite some time is building upon the strategic dialogue that we've had and building an operational component. We don't need to bring government and industry together just when something happens that we have to say, oh, my God. We need to do something now. We need to build in an ongoing, sustained collocation and collaboration between industry and government on this issue. Neither can do it alone and we can't do it in the midst of a crisis. We have to do it on an ongoing basis and we need to build the mechanism to do that.

MR. WINGO: Thank you. Ellen, do you have any thoughts on next steps and moving forward?

MS. DONESKI: Well, I think that a lot of what folks have talked about – Senator Rockefeller and Senator Snowe's piece of legislation that tries to pick up on different pieces of what you've talked about that tries to build in a place a cyber dashboard where there can be information sharing between the private sector and the federal government about the presence of threats and in advance of having attacks on private industry. But I know that there's a lot of skepticism about how that might work and when Senator Rockefeller wrote the bill, he was hoping that he would get engagement from the folks in the private sector to help us outline how we can actually make it work in the real world.

So I'm excited to have the opportunity to ask people to send us their comments and views as we trying to refine that legislation before we try to mark it up in the commerce committee.

MR. WINGO: Thank you. Richard, I want to ask next steps history, something I actually asked about. If you have any thoughts on that and also, what do you think about some of the most important things that the military could be doing as far as its role in moving forward?

MR. HALE: Okay. So let me just talk about my thoughts as a Department of Defense person. So we have three fundamental cyber goals in the Department of Defense, and they don't sound like cyber goals as much, but we need – so DOD has to work when nothing else will sometimes and so we've got to have dependable mission execution in the face of hostile cyber warfare or cyber warfare by a capable adversary. And the capable adversary is the important point. So it isn't just that we're worried about cyber crime, although we worry about that, but DOD has to work in the face of this threat. Now, a lot of other things have to work in the face of this threat too, but I'll be parochial just for a minute.

So back to the sharing with international partners and industry, this business of defining what a mission is quickly spills outside of the Department of Defense. Many of our missions are interagency and the rest of the federal government. Essentially, every mission is also a coalition mission with lots of other partners, either close allies or people we aren't used to doing business with, the Chinese for instance in piracy or earthquake relief for instance. So we have –

MR. WINGO: And Richard, by piracy you mean on the high seas.

MR. HALE: I'm sorry. On the high seas off of Somalia. Yes. Not cyber piracy or stealing Microsoft code and selling it again. But the other piece of it is that at least the communication infrastructure the department depends on is 80 percent commercial and so that mission dependability is clearly a joint government industry problem. We can't do this without close interaction with industry. So dependable mission execution is job one.

Job two is safe sharing, so DOD has had lots of security roles over the years so history – we made a decision in the '70s called "system hide," so it was a computer science decision, but it has shaped everything the federal government has done ever since.

And that is, we'll have separate top secret network – separate secret network and a separate unclassified network and once an atom of information gets into one of those networks, it's trapped there. So if it's an unclassified piece of information but somehow it ends up in the secret network, it's considered secret in this trap. So this is really inhibited information sharing. So the theory was if the security guys were the ones that cooked up this scheme to make information sharing hard, it had to be the security guy's problem to fix that. So safe sharing is problem two that we have in the cyber business.

And then problem three is that sort of traditional security problem. We still want to keep the secret some of the time and that's also a very coalition oriented thing. We may want to keep a secret within a particular set of countries. We may want to keep a secret very tightly just within a little piece of the Department of Defense. So coming up with structures that allow this, again, this ad hoc coalition formation and sharing while keeping a secret is another problem. So, again, the historical technology problem has been the system hide decision.

Just one other historical note – I think it's also clear based on events in Estonia and Georgia that cyber warfare is going to be a piece of the next big fight. So DOD has to take this seriously and it's great the president's taking it seriously and the secretary of defense is taking seriously so we have a chance – so that is different than it has been. We have a chance to tackle this.

MR. WINGO: Thank you. Phil.

MR. REITINGER: Could I take your invitation at the start to sort of have the panelists take over the panel because I'd like to –

MR. WINGO: Absolutely.

MR. REITINGER: I want to kick off and make sure we don't drop a point that Chris raised and that is sort of the human element, the education, the workforce, because these are all tied together. And we're – in full disclosure, we were having a conversation about this in the green room.

MR. PAINTER: Blue room.

MR. REITINGER: Blue room. Right.

MR. PAINTER: It was multicolored. (Laughter.)

MR. REITINGER: It was a lot of primary colors around this place. But it seems that this is not just a security issue but also a competitiveness issue. We're not producing in this country enough of the security talent, development talent that we need in order to both ensure the economic viability of our key private sector players and their security and the security of our country.

So I think we've got to revamp how we do this starting very early on, catching people when they're five or six-years-old and getting them excited about the possibilities of going into this space, doing coding, doing other sorts of things, much like, you know, years ago, you'd have kids out there with their moms or dads working at the engine of a car. It's the same sort of thing. You've got to get people excited, move them up and make sure that when they go into more development that there's security education early on, when they're in college that if they're taught how to do development or taught IT, they get the security fundamentals as a part of that, as Chris was saying.

And then once they graduate and go into the workforce, that we have mechanisms that give them career paths so they can have a full career. They're not stuck as, oh, you're the security guy. You're a GS-12. For those of you in the federal government, you know what that means. There's unlimited (means ?). You can go up through the SES; you can go through the political ranks as a security professional.

I think back – back when Chris and I were both line prosecutors, in the mid '90s, we had this problem where you'd see investigative agents in particular who would develop considerable expertise in doing cyber crime investigations. And then they'd be rotated out. They'd be doing some sort of paper fraud or something else. And some of them said, enough of this. I'm going into the private sector where my skills are in demand. That's changed substantially throughout the federal government but we've got to farther. We've got to make sure that we develop that career path and then provide the workforce training as people go forward. And I'm sure lots of other people have thoughts about that.

MR. PAINTER: And I think it's a career path especially it's something that's really important. One of the agencies that Phil mentioned, the FBI recently, cyber is one of their top priorities. And it used to be very much, as Phil said, you'd go into a little cyber, you'd go do something else, you do something else again. You can't really understand this field unless you stay in it and you play in it and the developments are too fast to go away.

And that's not just true in the law enforcement field. It's true in the network security field. It's true in the policy field. It's true across the board. They have developed

a career path within the FBI for this where someone comes in; they stay with it their whole career. They get more and more training, more advanced training. That's happening in the network security field in government. It's happening in other places but we really need to accelerate that. And I think Phil's right. We need to make this cool for kids so they actually think it's something they want to do.

MS. DONESKI: I would just say that on this point, I think there are a lot of aspects of cyber security where there'll be controversy in Congress I think on workforce development and training. It's something that there can be congressional encouragement of through scholarships and training programs and that it's also easily something that we can work with the private sector that's already got its own training. Google has its own training as well as other leaders in the field. So that's a place where we could come together, put more resources so that we're prepared for the future and it wouldn't run into any of the controversies that some of the other big pieces of this policy might.

MR. WINGO: And Ellen, you're right. Google does have training on this. In fact, for our engineers we continue education but we (bake ?) cybersecurity into everything that we do. And as Phil mentioned, we were having this conversation in the waiting room before and I found it fascinating the idea of actually getting kids involved. We teach Spanish, French, languages to kids. Well, why not consider code as another language that kids could start very early to learn how to do and then you just bake cyber security and awareness on top of it.

So anyone else have comments on the pipeline? I guess we would call this a pipeline issue. How do we get the cyber security professionals of tomorrow ready today?

MR. HALE: So I have one comment. There are some work examples I think that are models that we can follow. The National Security Agency has their centers of excellence program where they've gotten a lot of universities to put together a curriculum on cyber security and teach it.

The other thing we have is the National Science Foundation and the NSA scholarship programs that are graduating first rate kids who owe the government a little bit of time but what we found is they tend to stay in the government when we can give them good work. So they're transforming this bottom up. That's an incredibly successful program. It's probably the best money we've spent so far in cyber security. So I think we need to do more of that.

But the other piece is I do think we need some curriculum review. This technology is really fragile. I tried to make this point in the green room too. Everybody who writes software has to think about security. You can't just be security people who think about security. So this business of baking in security really has to start with the people who are doing the design of things and the coding of things. So every single computer programming class has to consider security as part of the computer programming class. It isn't an algorithm class and then a computer security class.

So my analogy is it's like doing civil engineering without worrying about gravity. Everything in civil engineering is figuring out how do you make buildings stand up and

bridges stand up and things like that. So human behaviors are gravity in computer programming. We've got to consider it in everything we do.

So that's a thing that I think the government might help influence. Partly, by the way, we fund R&D. Partly, by the way, we reward colleges and universities with R&D. You know, we might put some strings on it around curriculum development or curriculum change.

MR. WINGO: Liesyl.

MS. FRANZ: Again, I'm not going to disagree at all with anything that folks have said. The only thing I'd like to add is that as we look at ways to develop our cyber security professional base over the long term, and this is a truly strategic effort, right, is to think of it also in a multidisciplinary way. Absolutely yes.

You have to build up the very technical expertise of those that are going to be discretely working on building software projects or systems engineering or architecture, but keep in mind that all of us in this room now use computers and other devices so back to what Chris said earlier about the human element or Phil – both of you probably said it – about the human element. Let's not just look at it as a technical – not just a technical training but also multidisciplinary efforts to build practices and norms and awareness and the kinds of things that we as individuals need to do at a very young age as well.

Also, I would say that not everyone that's working on cyber security today has an engineering degree. So I would like us to think in as flexible terms as possible, not only for the types of people that might be touching cyber security in their company or in their government organization but those that can contribute to a multidisciplinary and ever evolving technological environment. So let's try to keep some flexibility into it for that evolution as well.

MR. WINGO: Thank you. One thing I'd like to ask is on the one point made in the 60-day review was importance of public-private partnerships. And so on the private sector side of this, what is collaboration look like if you have an incident where you have incident responses? I'd also like to loop into this question there's legislation that proposes the idea of having an – shutting the Internet off from critical infrastructure. I'd like to get your take on how would that work in practice, for example.

MS. FRANZ: Maybe I'll take that as the private sector industry I represent here today.

MR. WINGO: Liesyl.

MS. FRANZ: First, I think I touched upon what collaboration might look in an incident and the key part of that is it's not just during an incident. It's in the collaboration, cooperation, collocation, co-analysis. A true partnership from day one, really, so that when something happens, there is an organic way to respond, not a forced way. You're not just reacting. You've developed a proactive approach to addressing a problem by working together over the long haul.

With regard to a disconnect kind of proposal as suggested in the Rockefeller-Snowe bill, I would say that we really need to have a strong dialogue about that kind of thing because, first of all, it's not something you can just do. I think in today's technological environment, you can't just disconnect somebody without either unintended consequences for the services that that network provided or the fact that there are all kinds of redundant networks and ways that people continue to do business so even though you might have disconnected one thing, you've not disconnected another.

So you really have to sit down and have a dialogue about what actually would happen if you did that. And I would say that perhaps there might be alternative measures to protection and emergency efforts that might be needed.

MR. WINGO: Ellen, I'm absolutely going to give you a chance on this since it's the Rockefeller bill, Senator Rockefeller's bill.

MS. DONESKI: Thank you.

MR. WINGO: But actually I wanted to get the perspective from the DOD on this as well as Phil, maybe both of you on this issue of incident response but also cordoning off private sector infrastructure from other systems and how does that all play out.

MR. HALE: So I'm an old guy in DOD now so I have some ancient history stuff that I think actually might be helpful as we think through some of this. So when AT&T broke up, DOD said, hey, our com infrastructure is no longer owned by one company. The country actually said it's a national security priority to be able to work with industry if there's some problem and we've got to be able to work across the whole industry that handles telecommunication.

So there was an outfit that was formed after the Bay of Pigs, actually was sort of a telecom emergency thing, the National Communication System which is now part of DHS but after the AT&T breakup, there is this National Coordinating Center, I think, was called, and it was actually manned by people from all of the telephone companies and by DOD people and by intelligence people. So we actually had a full up operational entity and it still exists.

I think the priority has gone down a little because cyber has overwhelmed this a bit, but we had a model where we could operate very quickly in an emergency and we used it. So in 9/11 it was used heavily, for instance, to try to figure out how to restore – the president's priority was safety, you know, rescue people and then get the stock market running again. You know, the NSC was the entity that helped coordinate those priorities and coordinate the actions by industry and government so we're all working together toward those goals. So something like that I think might be important.

Another sharing thing that started is – DOD started worrying about its technology secrets leaking out of its industry partners' networks. So big defense contractors pulled all the technology data for the department. They were getting cyber attacked as well. Data was being exfiltrated from their networks.

So the department started another thing that I think that might be a bit of a model called the Defense Industrial-Based Cybersecurity Effort and we started to wrestle with these thorny problems of how do you have a really tight sharing relationship with somebody that you also want to compete for business from you. So this is one of the problems the government has.

So how do you work that, and how does industry respond to that in other – we want them to share incident information. They don't want it to be used against them in the next competition for a fighter plane for instance. So we have a really robust pilot project right now with about 30 companies where we've worked through the legal arrangements and we're proposing some federal acquisition regulation changes to enable the sharing.

But the thing that the industry folks came back with and said, fine. We'll tell you incident data but you've got to give us something. What are you going to do to help? So we have always shared best practices through NIST or through some DOD entities or through NSA.

But we started sharing threat data, classified threat data in some cases, and this is a big breakthrough. We haven't done this in the past and I think we need to grow this model and the government needs to have – this is a conversation we need to have internal to the government: how classified does some of this threat data need to be and how widely can we share it? So can we share it with the banking sector? They need to understand some of this stuff that something's coming out and we want them to be robust too.

So we started this with this defense industrial base. It's actually been under the critical infrastructure protection laws. So you know, we think it may be a model that can be grown out and inherited by DHS to have this broader conversation. So I think only answered the first part of your question but I've gone for a long time.

MR. WINGO: We'll let Phil answer the second part. This is the issue of having a

MR. REITINGER: Actually, I'm going to stick on the first part too. I want to start where sort of Liesyl left off. I mean, the first point is there can't just be partnership around incident response. It does have to be partnership more generally because it's got to be built into the DNA of all of the different players because when – if something bad happens, the last thing that somebody in the private sector is going to do is reach for the 300 page government binder on the shelf behind them. That's just not how they work. They're going to start doing what they do on a normal basis, but scaling in their best way to meet the emergency. So we've got to build those organic ways of working together.

As Richard said, we don't start from scratch. There are a lot of models out there; the national coordinating center model which goes back to the early '80s as he pointed out is a very good one. And in fact, that particular model of what amounts to a joint operation center between government and industry is behind a lot of the proposals that you see coming out of bodies like the NSTAC that some of you in the audience were deeply involved in developing, two in the front row.

So those ideas don't go away – and there's the DIB (sp) model too. We've got to figure out the way that we refine those and help them to meet what is a broad cross-sectoral issue. And I'll say, there are at least – we can spend the rest of the panel literally talking about public-private partnership and information sharing. I'll call out sort of three things that I think are absolutely essential.

The first is trust. You've got to have trust. With trust almost everything else will work and without trust nothing will work. So you've got to build that. You've got to start with personal trust and you've got to move towards organizational trust where in that – you know, there's a return on investment for everybody involved so they continue to play in that partnership.

And as Richard said, that involves on government making sure we share the information that we can share, not overly classifying information. Or, if necessary, providing the right security clearances to people in industry so that they can see it and making sure that we give them information that's actionable, not, here's some highly classified information. By the way, you can't do anything with it. So that's not particularly helpful for people in industry, except to generally inform what they're going to do in response to the threat.

The second thing is agility. You know, we built a lot of mechanisms to work together, the information sharing and analysis centers, the sector coordinating councils, the various advisory committees and the bodies that go along with them, the national coordinating center.

All of these and more are designed to work together. We need to work through them where they're working but we also need to have an ability either through them or otherwise to bring together the right people in a very agile way because you can get unique problems, you can see a vulnerability coming that affected three companies in there for multiple sectors. And you need to bring together the right people to solve the problem very, very rapidly.

The last thing is clear roles and responsibilities in sort of a light process for how we're going to work together. That goes back to pulling – nobody is pulling that 300-page binder off. We need to tie down, as part of the incident response plan that should come out of the 60-day review who does what, what are the roles of everyone, how do they implement that in their existing business processes, whether those are government business processes or industry business processes, so that we can all work together without trying to build the plane as we're flying it while bad things are happening.

MR. WINGO: Thank you. Ellen.

MS. DONESKI: That's actually a perfect place for me to jump in because I think the provision in the legislation, the Cybersecurity Act of 2009 that Senator Rockefeller and Senator Snowe introduced in an effort to get exactly this kind of dialogue going. We didn't envision it as any kind of on/off switch. Probably the terminology in the draft is imperfect and we need to change it because we only are speaking to lines of authority so that we know what happens in the event of a cyber attack so that people aren't guessing so we don't have the kind of situation and confusion that we had with Katrina or 9/11 where there's

confusion between the national decision makers and the local and state authorities. It's really about trying to make sure that organically there's an understanding of who does what.

And I think we were trying to state the obvious that in an extreme cyber emergency or attack, the president ultimately has constitutional authority to protect the country. It really wasn't meant to go beyond that and this kind of a discussion is something that we've been having in conference rooms since we introduced the bill and is very helpful in this interim process that is legislation so that by the time we get to actually moving the legislation I'm hoping that it will be more warmly received.

MR. WINGO: Chris, if you –

MR. PAINTER: I think a core part of the report too was exactly that, defining what the lanes of the road are and how these agencies on the government side work together and how they work with the private sector. We've known this has been a problem for some time but we really haven't had a robust incident response plan. That, of course, is only one part of the public-private partnership.

The way I thought it out – and I really echo most of the sentiments Phil's and others' that have been mentioned here – but partnership for what purpose? People throw around the terms public-private partnership all the time without any real content behind it.

So what's the purpose of the partnership? Is it incident response? What relationships do you need to develop? What do you need from industry as government? What can government give to industry to make that value proposition important? Getting people to report to you incidents, that's always been a big problem. It's been a big problem for as long as I think any of us have been in this area.

But one of the reasons for that is the people who were asking to report don't really see what benefit they get out of it, so making that value proposition clear which I think is a government and industry problem. We need to do our part too.

I don't think – to echo Phil's point – I don't think government necessarily is going to be picked up in a big cyber incident and get the 300-page thing off the shelf either. We need to have – to find lanes in the road organic processes so we can come together and really respond. That's one of the things we're working on.

MR. HALE: Can I ask Phil a question?

MR. WINGO: Absolutely. Please, Richard.

MR. HALE: So DOD, what we do is we plan. We are a planning outfit. We plan everything. We work out relationships and in spite of all that planning, what we discover is there's no substitute for practicing your plan. All those details that you didn't think of appear in that practice. So, Phil, what do you think about how we ought to work out – we have some legislation that defines some lanes but how should we really work that out in practice?

MR. REITINGER: Sure, Richard. I agree with you completely. One of the reasons DOD exercises and practices so much is because the idea is that one is not in war normally. So you want to train and practice to what you're going to do.

In some ways, cyber security is a little different because one is always in that environment. We are – every one of us, all of us, are always under attack. So are in slightly different place and events happen all the time.

For example, telecom companies, they get cable cuts all the time because of a (vacuum ?) that just dropped somewhere. So what they need to do and what we all need to do is to be able to scale rapidly to address situations that can much more severe than what we do on a day to day basis, and in cases where it's a really an uptick, maybe that's a different of kind and not like.

So we actually do need to – even if we didn't want to, we do need to exercise to plan for that. We've done a series of exercises overtime, cyber storm one and cyber storm two and cyber storm three is in planning plus there is a whole series of exercises in both government or government and industry to make sure we're getting ready for future events. We need to do a couple of things.

One, we need to first off continue to do those things, make sure they're not too burdensome so they keep people away from doing their day to day job, but make sure we do them and do them to the right way and get the private sector, where appropriate, involved from the very start so we are in fact training to the goal and bringing all the people in who need to play.

Second, we need to make sure that there's a cadence around those exercises so we are using them in concert with our policy development and testing the things that we actually want to use. So as we go forward on exercises, we want to make sure those align with the incident planning and response processes that we're developing and that we've got an interim cycle, much as DOD has always done, so exercises inform plans, we exercise plans and we actually loop through around, and included in that is sort of future planning. What do we think we're going to need, what capabilities will we need in three years and five years? Design the plans to address those, the capabilities to address them, exercise and look around for a cycle of – you know, a virtual cycle effectively.

MR. WINGO: At this point, I'm just going to ask one more question but I'd like members in the audience, if you'd like to start lining up at the microphones, we're going to take questions and also from Google moderator after I ask this one last question.

A great point was made – I think Chris and someone else mentioned – what's the flow back to the private sector? In other words, sometimes, there's a question, we give up information. If you're a business and you say, what's in it for us, how do you share, and so it's great to hear that folks are really thinking about how do we provide that value, how do we send information back and figure out a framework that we can work together to make sure that that's working.

My last question from the panel before we take questions from the audience and Google moderator is what do you think in a concrete sense we can do to really get the word

out and involve citizens just in the sense that there is of course a criminal element to cyber security and the problem as well as small businesses, the impact – you buy an expensive computer. Maybe you have several, if you're a small business person, and they're fried. You can't use them and then just – this is – people are becoming more aware but what's the role for this really public facing, consumer side of this effort?

MR. PAINTER: I think one of the chapters, a full chapter in the report was based on both the education but also the public outreach and a real public outreach campaign that is supposed to educate the public about how important this issue is.

And one of the things I've seen is that you know, a while ago at least, we had to change the culture. A lot of people, kids growing up think that being a hacker might be cool, attacking things might be cool, that there's not really anything wrong with that. It's different from someone breaking into your garage next door because it's in cyberspace and they look at that differently. I think that's changing. We need to accelerate that change.

With small business and other business, in terms of reporting the intrusion, not just the law enforcement but to the network security experts, I think as they see these really impact their bottom line, that's something that becomes important and they understand that by contributing that information, they may not be the only victim. That's a whole lot of other victims and you can only get a sense of the problem and do something about it if they come forward.

What we have to do is convince them of the capability we bring to them that we can actually do something for them and I think there is, not just in the law enforcement side but the network security side and the policy side and especially dealing with things that maybe they can't do like deal with our international partners since these always have an international dimension.

MR. WINGO: All right. We're kind of running out of time so unless there's – Phil.

MR. REITINGER: Briefly, this is something of sort of a hump problem, right, because what we're got now is a collection of people who did not grow up with IT sort of embedded in the infrastructure and everything they do. Now people grow up and by the time they actually take their drivers' test, they've been around cars and seen people driving forever and they've taken driver's ed in high school probably. So there's an entire – the entire community informs them, educates them about driving from when they're very young. We'll get there eventually if we do this right. But we've got to get over that hump. We've got to get to that point. And that's why the recommendations in the 60-day review are so important.

This is not a blank slate. People have been doing great work like the National Cyber Security Alliance in this space for a long time, but we do need to step this up to another level. We – if in fact, as I believe, this is a national and homeland security problem, then we have to treat it that way. And we've got to make sure that we devote the resources and the effort to really educate the public down through kids, through individuals, through small business, and through corporations as to what the threat really is and what they need to do to protect themselves.

So this is – it's not a mystery what we need to do. We just need to execute.

MR. WINGO: Thanks, Phil.

MR. : And that ties back to the president's statement. This is a national priority.

MR. WINGO: Right. Now we can take questions from the audience and our Google moderator. If you could please just introduce yourself and then ask your question briefly.

Q: I'm Michael Nelson of Georgetown University. I think this has been a very useful panel and very encouraging. You've laid out the right issues. There's a lot of agreement on this panel about what needs to be done. But I've been a little frustrated that we haven't spent enough time looking at how to make the infrastructure itself more secure. And particularly, I wanted to pick up on Phil's point that we need to have, at its foundation, an infrastructure that has good authentication built into it with privacy protection built into that authentication mechanism. When Phil and I and others were working on cyber policy 15 years ago in the Clinton White House, we all knew that we had to have better authentication. And 15 years later, we have more problems with the online identity theft. We have more problems with phishing. We still haven't solved that problem. There have been dozens of private-public partnerships.

To highlight some of the specifics in this area, I'd like each of the panelists, or whoever wants to take it, to tell me why you think we haven't made progress on this fundamental issue in 15 years, and what we need to do going forward – industry, government, Congress.

MR. WINGO: Richard, do you want to –

MR. HALE: So what I'd say is – being old again I got to watch all these technologies develop. All of these technologies were developed with the notion that everybody was benign and they were all developed with the notion of anonymity. So the network is completely anonymous. There is essentially nothing built into the technology infrastructure that makes it less so. So in the department, we have a goal, underlying some of these higher level goals I mentioned, of driving anonymity completely out of our internal networks and with as many mission partners as we can. So we're struggling with the privacy problems. We've decided things like social security numbers can't be part of that. We've also decided that technologies can involve long, lifetime secrets. And again a social security number somehow turned into a long, lifetime secret.

When I was a kid, we printed them on our checks. They weren't secret, right? The Privacy Act made them secret. So we've pushed aggressively in technologies that don't require us to reveal authenticators, yet allow us to authenticate. So we have a big public infrastructure on the unclassified networks and we're rolling it out. And we have a big one on one of the classified networks and we're rolling it out on the secret network this year. I think those kinds of technologies have to become much more ubiquitous, right? We've got to drive out the anonymity.

The other thing we've struggled with, and back to the "it's not just a technology problem" point, is as you drive anonymity out, you still need to figure out how to establish enough cues so that people trust others that they've just discovered. So now, I know it's Richard Hale, so what? Do I want to do business with him? Do I want to interact with him? So the other structures that need to come around, learning other things about Richard Hale, in a dependable way – and this is the trick, right. It can't be easy to mess with that information either, so you can make a business decision around Richard Hale.

So what I'd say is I think there are technology pieces, parts to start to solve this problem. Again, we've worried a lot about privacy as part of doing this. I don't think we've solved all the privacy problems, but some of this business of not revealing certain information in order to authenticate is part of it. But I think the pieces are there. We just haven't had the economic reason to do it, except in places like DOD.

MR. PAINTER: And I'd take off that statement. I think one of the reasons you haven't seen it is the business case has been made to the industry or to the public in terms of – as it is today. Now, people are losing their identity and they see the identity thefts and these data breaches. I think it brings it more at home to them. I think the other issue is: how do you build in the privacy and civil liberties into this debate? And I think it's very important. I think that there are some purposes where you need anonymity, and some where you need more authentication. In fact, if you have a good authentication, you really do this right, you're enhancing privacy. You're protecting people's data and you're making the pie larger, rather than doing a zero sum game. And I think that's important too. One of the things that, I think, really was unprecedented about our report and the structure going forward is the civil liberties and privacy of a person is going to be a part of the NSC directorate that's dealing with this, with all these issues. And so we're really going to have that kind of dialogue to make sure we balance the equation correctly. But I think there's a lot in this area that can be done that would really help get all the noise out of the system and make us more effective.

MR. REITINGER: So – since it's my point, I'll say something, specifically on why I think the problem is. The problem is policy. It's not the technology. Technology's been there since 1995 or well before. First off, I would disagree perhaps slightly with Richard that I don't think the point is driving anonymity out of the system. The point is making strong authentication available for places where it's appropriate. And that may be on a DOD network everywhere, but on the internet it's certainly not. And we have to recognize – vis-à-vis Chris' points – that anonymity is not only highly socially valuable, but constitutionally protected for a lot of the stuff that happens on the internet. So we have to keep that very much in mind, but at the same time, making it easier to have strong authentication.

Why we haven't made progress is, I think, it's not – it's not a public good problem. It's a bit of a collective action problem. Too many pieces need to move together at the same time for this to have happened organically. Maybe some industry, or some entity in an industry, wants to use strong authentication, but because there's not a broadly available way to do that, they've got to kind of roll their own. And it's not worth their economic dime to do that. And governments never really provided the ways to optionally authenticate online if you want to do it. And so there's just – the people that could act don't really have the incentives to act. What – where we've got to get is we've got to get to the point where,

if you don't want to use things like a username and password, a set of shared secrets – they may be shared, but they're not really secrets – you don't have to use that. You can use some sort of credential that provides you much more authentication or much greater degree in security. If I want to see my first savings plan or my IRS information or something, then I've got a strong means of authentication, so I can have the security to do that. I can optionally do that. And so I think how we get there is find those places where we can catalyze action by government or industry and spiral outward from it.

MR. WINGO: Liesyl?

MS. FRANZ: I think we addressed the first part, which was how do we get more use of technologies that are available already. I think if truly there is a place where the market hasn't met a need, then perhaps we can look at a way for another public-private partnership to bring resources of government and the resources of the private sector and whomever else needs to be involved together for a specific project that might address more fundamental things, where there isn't a current technology or it isn't a current system to adjust your infrastructure point, Mike.

MR. WINGO: Thank you for your question. Over here.

Q: My name is Steve Grandson (sp) with Terrorism Research Center. This may be a question for Richard. We've received some reports recently through cyber security experts testifying on the Hill that China has developed its own secure operating system and it's been developed in the past six years. And they just started deploying it in 2007. Is this something that the DOD is doing? The reason I ask is it seems like we're kind of under the reactive instead of the proactive here. The DOD has spent over \$100 million apparently in the last six months on cleaning up cyber security issues and what not. Do you think going forward we can continue to partnership with some of these private entities where their focus may be more on business developing and really not security in some of their products? Should we be developing our own security software like the Chinese have done?

MR. HALE: Oh, man, this is another old guy question. So back in the system high era, the DOD did make the decision that current models for operating systems, in particular, were not sufficient for this problem of both handling multiple classifications in a single machine, but also just for general resistance to cyber attack. So we wrote a guide book on how to write an operating system that was more resistant and then handled thee labels and access control based on the labels. And we had a public-private partnership thing going. We had a really, really great one. We had every operating system in the world essentially, except for Microsoft, build one of these operating systems, and then we massively non-adopted them. So now we've burned industry. People looked at that and said, "I'm not spending money on that again. You guys promised that if we made these, you would make a market for them." So I think there are a couple of lessons there.

One is, yes, the government does have to be more active in demanding an infrastructure that's more robust. The government is going to have to pay for it. Now, so if we can use our collective buying power, the government is still a big information technology customer. We can actually help nudge the market at least. We can't completely shape it anymore. So I think we have to be much more serious about using our buying power to harden up some of the commercial things. And yes, there are places we're going

to have to build our own special purpose technology. We still do it – cryptography, there are going to be some other infrastructure pieces the government's going to have to build itself.

MR. WINGO: Okay, next question. We have 15 more minutes, so what I'm going to do is try and move through as many questions as we can. I'll probably take two more, and then go to a moderator question for the panelists. I may actually cut off after one or two, but if we have extra time, please keep in mind the questions you want to revisit.

Sir?

Q: Brian Rowe with Public Knowledge. When I hear the rhetoric of “we're under attack at all times” and security, along with my geek background, it's very difficult for me not to associate those things with warrantless wiretaps and telecom immunity or mandating that printers print out information in the pages that give up individuals' information about who printed that information. So what is going to be done, no just to give lip service to privacy, but to ensure that these programs are open and transparent, so that we the citizens can decide whether we want to give up those rights in the name of this war that's being put forward?

MR. REITINGER: I'll just start by saying I don't think you should be asked to give up rights. I think we ought to find ways to move forward. I don't want to sound just like lip service, but I really mean this. We need to find ways to move forward and protect security and privacy at the same time. There will be places where there'll be push points, but I think in a lot of areas we can do that. We obviously need transparency to the greatest extent possible so that we can provide oversight from the public about what we're doing.

The last thing I'd say is that, as Chris pointed out in response to the question earlier, the 60-day review specifically said on the team, on the cyber security team, in the White House there's going to be a privacy and civil liberties person present. And so we've got to institutionalize the perspectives that we need in order to protect privacy. I think you would find that during the course of the 60-day review that the outreach that was done broadly by the team that did it under Ms. Hathaway's leadership was extremely broad and included the privacy community. And I think that was – that was a very lights on fact for a lot of people in the community.

MR. PAINTER: And that's absolutely right. We've met with many of the civil liberties and privacy experts several times. And they were delighted by it. They said that's something they really didn't have that experience with before. So it's really more than a lip service. This president has made transparency a bedrock principle of his presidency and something that we take very seriously. And we want to make sure that when we're looking at all these issues, we're building that in.

MR. WINGO: Brian, thanks for your question. Here?

Q: Hi, my name is Ian Crone. I'm representing the Center for Advanced Defense Studies. I'm curious in a situation in which we have civilian, military, and private networks all running on shared operating systems, and not just our own networks, but also those of our potential adversaries, how do you build that relationship and that balance between a

potential offensive capability with the military in developing and researching offensive applications? We have this new cyber command. How do you balance that against the need for defense? If we discover a vulnerability on side of the public-private divide, especially on the military side, how will that information be shared? Should it be shared? So do you patch a vulnerability or do you keep it secret to exploit?

MR. HALE: Is that one for me? Yes, thanks. (Laughter.) So I think it's a great question. Right now we tend to share the vulnerability information we find. So I can't talk about some of how these processes work because they aren't public processes. But there is a vigorous debate process inside the – actually inside the whole federal government – it's not just the Department of Defense – about how this should work. and in general, the way it works is we choose to share the vulnerability information and fix whatever the vulnerability were, at least encourage to fixing the vulnerability. We do have a very active program to do that. And we've also tried to catalogue these things and share them as widely as we can. There's something called the National Vulnerability Database that is run out of the National Institute of Standards and Technology, where a lot of this vulnerability sharing is done.

MR. WINGO: Liesyl?

MS. FRANZ: I think an important aspect of that is the ongoing dialogue that I mentioned between the various parties on an ongoing basis, not just when something happens. And there's also the notion of responsible disclosure that has been worked on over time between government and industry about how to disclose something at least publicly that at the right time, when it allows people to action to defend themselves, but also doesn't subject the environment to being slated and without some protections being put in place. So I think there's a lot of dialogue required and a mechanism for that on a consistent basis.

There's going to be times where there tension between a disclosure or not. And that just needs to be worked out as quickly as possible. There have been instances where the traditional ways of disclosing have been overruled by the dialogue that took place.

MR. WINGO: Thanks. So I'm going to get the Google moderator now. Actually I might combine the first two questions. How will the lack of international law by treaty or a precedent on cyber warfare affect U.S. development of cyber defense capabilities? And then also, has the Defense Department outlined a moral framework for offensive cyber warfare? Could concepts like preemptive war and mutually assured destruction apply to cyber space? Anyone wants to jump in on that one? Richard, we could let you also off the hook. So why don't we hear from someone else that got – unless you want to jump in?

MR. HALE: We're lawless. I'm not a lawyer. So I say one of the lawyers should – (laughter).

MS. FRANZ: I'm not a lawyer either, but I would just say that I don't think we need to wait for a treaty which might not be optimal anyway to start – to – excuse me – work on defensive protective measures.

MR. PAINTER: Right and I would say that one of the things we talk about in the report we need to do is to work with the international partners to try to define what some of the norms are in cyber space. But one of the things I think that's also clear, when we look at all these events that have happened, is there is a fundamental thing we need to do, no matter what the attack factor is. And we have threats from criminals, from nation states. There's a whole range of threat actors out there. We still need to do certain core things. One of those things is to harden the targets, make sure we had the defensive measures in place, make sure we have the incident response plan in place, make sure we had the partnerships in place, both internationally and the private sector. Those are all core no matter what because attribution is still a big issue in this area. We don't always know who's doing what to us and we need to get better at doing that too.

MR. WINGO: Just real quick, Richard. I want to mention one thing. We talked in the waiting room, a bunch of us, about maybe a loose analogy, which is not the same case, but for piracy on the high seas. It's also an international problem that's age old. Just in the spring, the Maersk, Alabama, 350 miles off the Somali Coast was attacked by pirates. Richard and I were both in – had Navy connections. I used to be a frogman. So that was ended with the application of force by Navy SEALs, but the development of both international norms, cooperation, and also the private sector. I was just watching a documentary on what happened and the procedures that these vessels have. They share amongst themselves best practices. I think one of the first things they did was call some antipiracy center in the UK, when they were being attacked. So on this question I thought it was interesting. You've talked about history quite a bit during this, so Richard, what are your thoughts on this question?

MR. HALE: Well, at least for now, we've been trying to cook up as many ad-hoc relationships as we can. Some of them are very enduring relationships with our closest partners. Those relationships have been in place since before World War II, for instance, and we've used those relationships to expand sharing around cyber stuff and around incident response. We've succeeded in some of the cyber emergencies in putting together ad-hoc coalitions and partly what DOD does for a living is put ad-hoc coalitions together and figure out how to get something done around some of the cyber emergencies in other parts of the world. So I do think we need a better – there aren't social norms here yet. I do think we need better notions of what those are, where the boundaries are, and again, maybe this is back to the roles and responsibilities conversation. We need to figure some of those out with our partners, so it's not all ad-hoc.

MR. REITINGER: One quick point. This is another area where we need to go farther, stronger, faster. As the 60-day report makes clear, this is inherently an international problem. We have to solve it internationally. This is something no one government could solve. Let's not – while acknowledging that we've got a lot farther to go, let's not pretend that nothing has happened. Both Chris and I have served time chairing the G-8 Subgroup on High-Tech Crime and many, many years ago, in internet time, probably a century ago, the Council of Europe developed a Cybercrime Convention, which was the first sort of major international instrument and is a very effective way for law enforcement around the world to work together on a very rapid scale to solve crime. Now, that needs to be adopted much more broadly internationally. One of the things the Senate did a few years ago was to ratify that convention. That was a very good thing. We need to find ways to build on those successes, but successes they have been.

MR. WINGO: Thank you. Question?

Q: Matthew McHale, Public Knowledge. So earlier someone mentioned the idea that we need to bake security into the process of creating our digital infrastructure, our applications and software that are used on a daily basis. I think that's a wonderful idea, but I'm curious as to how any of you would – what ideas you have for implementing that. My own experience in the private sector is that it's not a lack of competence on the part of the programmers, but rather a lack of time and money. When deadlines loom, security is one of the first things to fall by the wayside. And it seems like there needs to be some kind of incentive to prevent that from happening because it's a systemic flaw in the software design process. Do any of you have any insight into how you might approach that?

MR. PAINTER: I think incentives are one thing we're obviously looking at. I also think the market is changing to some extent too. If software is more secure, it might demand a little bit of a premium because people don't want their information taken and they start relying on this information every day. So I think it's a combination of incentives and also the market actually valuing this more. I think on the government level, it's actually having the security people in the same room as the innovation people when we consider these issues. So they're not two separate camps, but they're integrated and they're exchanging information at the outset.

MS. DONESKI: But the government could help drive the innovation in the private sector if it offered substantial incentives. And I think that's something that the folks in the Congress really are very interested in doing, and I think it's something that might be – take the form of a tax incentive. We're looking at all those options.

MR. REITINGER: If you want to bring the market to bear, you've got to have the ability for people in the market to make effective decisions. So you've got to be – let them make decisions based on data. And if you can do that, then you're going to bring a lot of additional incentives to bear too.

MR. WINGO: We can take one more question. A quick thought –

MR. HALE: Let me finish that thought. The government still has a lot of buying power and if we band together, we can actually make a market for some of this stuff.

MR. WINGO: Thank you, one last question.

Q: Thank you. Shannon Kellogg with the EMC Corporation. One quick point and then a question on the international front. The quick point is I agree with you on the authentication identity management issues and I think Mike's question was an important one. One thing I would throw out there on that front, though, is that there is a lot of focus on what's happening in government. There are sectors like the financial industry that actually have, for a number of reasons, some of it because of threat, financial laws, some of it because of market conditions, and then also even the government push, if you will, have actually gone out and adopted based on risk of those transactions a broad set of authentication methods. So I'd encourage you to look at what the financial industry is doing on that front. But the question is – I agree with what you've been talking about in

terms of the importance of international coordination, but going back to Phil's point about competitiveness – and Ellen, perhaps this is something that you might want to start off because I think it ties into the legislation the Center Rockefeller has introduced, and that is what about the international implications for what we do here at home, okay? And so there are different legislative approaches that are out there. There are different procurement requirements and strategies that are out there. There are a number of things that we're looking at doing in the context of the cyber review that could have an impact on how we're perceived internationally and could give some governments who are already starting to go in a direction and putting additional requirements on big companies and other multinational actors who are important to the American economy that are putting these requirements potentially on us that would restrict our ability to compete abroad. And so I'm just wondering, as you think about this challenge internationally, are you also looking at how policies at home can impact our competitiveness on the global front?

MS. DONESKI: I think it's a fair point, but I also think that it's incumbent on us to try to move the private sector to engage so that a government mandate is not required. Nobody wants to put a mandate on the private sector. Everybody wants to work on the public education and public awareness campaign and try to make it something that's part of the cost of doing business in the 21st century. That's where it ought to be. And of course, you always consider domestically what you do, how it might affect our international partners, but we think cyber security and improving our nation's cyber security is actually fundamental to our competitiveness. If we don't do it, it's going to result in some situation where the economy is destabilized because of cyber insecurity, because of cyber attacks. So we think it's a competitiveness issue to push the private sector to do more and do better, just as government needs to do more and do better.

Q: I agree with that point, but one implication is that there are governments abroad who are also looking at what we're doing to give them an excuse to actually go down a path that would be harmful to us.

MR. PAINTER: Well, and that's what it's going to get to. It's a flipside too. It's what we do here, but what is happening on the international community that affects businesses in the United States. And we need to – part of our international engagement strategy is to bring industry along. Phil's absolutely right. We've made huge strides in some areas like the Council of Europe, which is still – that treaty is still a cornerstone of our foreign policy, getting other countries to adopt that. We've built a lot of networks on some levels, but bringing industry into a lot of these discussions we're having with other governments to make sure that we have all this multiplicity of forms dealing with these issues. We're actually making use of them in a way that helps all of us together achieve the competitiveness you're talking about.

MR. WINGO: So Google takes cyber security seriously. We look forward to working with others in industry, members of the public, but definitely with the government as well. And we're attacked every day. It's a serious issue.

I'd like to thank each of you for your participation and it's a great panel. And to everyone in the audience, thanks for your time and your interest.

(Applause.)

(END)