THE BROOKINGS INSTITUTION

BUILDING TRUST IN THE GLOBAL SUPPLY CHAIN

Washington, D.C.
Thursday, April 18, 2013

PARTICIPANTS:

Welcome:

DARRELL M. WEST
Vice President and Director, Governance Studies
Founding Director, Center for Technology Innovation

Identifying Best Practices:

JON BOYENS
Senior Advisor for Information Security, Computer Security Division
National Institute of Standards and Technology

JOE JARZOMBEK
Director for Software & Supply Chain Assurance, Stakeholder Engagement & Critical Infrastructure Resilience (SECIR), Cyber Security and Communications (CS&C)
U.S. Department of Homeland Security

JOHN LINDQUIST
President and CEO
EWA Information and Infrastructure Technologies, Inc.

SALLY LONG
Director
The Open Group Trusted Technology Forum

Building Trust in the Supply Chain:

SANDOR BOYSON
Research Professor and Co-Director, Supply Chain Management Center
University of Maryland, College Park

EDNA CONWAY
Chief Security Strategist, Global Value Chain
Cisco Systems, Inc.

PAMELA PASSMAN
President and CEO
Center for Responsible Enterprise and Trade

ANDY PURDY
Chief Security Officer
Huawei Technologies USA

* * * * *

P R O C E E D I N G S

MR. WEST: Good morning. I'm Darrell West, Vice President of Governance Studies and Director of the Center for Technology Innovation at the Brookings Institution, and I'd like to welcome you to this event on the global supply chain.

Our forum is going to explore threats to the Information and Communications Technology supply chain and ways to identify best practices, standards, and third-party assessments for supply chain assurance.

As trade grows more globalized, supply chains have become increasingly complex. Contemporary commerce involves hundreds if not thousands of individuals, organizations, and technologies across multiple continents, and so we now are faced with new and unique vulnerabilities and threats.

This morning we are putting out a paper on 12 ways to build trust in the ICT global supply chain. It addresses a variety of operational and technological threats. I argue in the paper that there are a number of unpredictable threats ranging from natural disasters, geopolitical disruptions, an economic shocks to denial-of-service attacks, spying, counterfeiting, and system control threats.

As part of the research leading up to the paper, I undertook a series of interviews; we conducted a workshop with leading experts; and we've reviewed documentary evidence on supply chain risks and remedies. Based on this, we propose 12 ways to build trust, and this includes suggestions such as developing standards; using labeling and tracking chips to improve monitoring; deploying identity verification systems; relying upon independent assessments; certifying promising procedures; and accrediting strong performers. We think that these represent promising ways to deal with the threat. There's no silver bullet, but there are a number of very specific and concrete steps that we can take that we believe would make a difference. So, for additional details I'll refer

you to the paper on our recommendations and why we reached those.

To help us understand these important issues, we're pleased to welcome a panel of distinguished speakers. So, we have two panels this morning. The first one is going to look at best practices, while the second one will focus on ways to build trust.

For the first panel, I'd like to welcome Jon Boyens, who is a senior advisor for information security of the Computer Security Division within the National Institute of Standards and Technology. Jon leads a NIST supply chain risk management project, and in it he helps to evaluate tools, techniques, practices, and standards useful in managing risk in the ICT supply chain. He co-chairs a working group on the White House's Comprehensive National Cyber Security Initiative, and he participates in a variety of national and international efforts to develop standards. He has conducted research into the technologies that help enable organizations to manage the supply chain risk and has helped to develop some practices for federal agencies on managing their particular risk.

Joe --

MR. JARZOMBEK: Jarzombek.

MR. WEST: Okay, I was going to have difficulty pronouncing your last name. Hereafter he will be known as Joe.

Joe is the director for Software and Supply Chain Assurance within the Office of Cyber Security and Communications of the Department of Homeland Security. In this role, he leads the government interagency efforts with industry, academia, and standards organizations in addressing our security needs. He has worked in the cyber security industry in a variety of different ways, and prior to his service in GHS he worked in the Office of the Secretary of Defense.

John Lindquist is president, CEO, and chairman of EWA Information and

Infrastructure Technologies. He's held several security and privacy positions in various organizations, and prior to entering the private sector he served in the U.S. Army for 20 years.

Sally Long is the director of the Open Group Trusted Technology Forum, which is an international forum of industry and governments working together to increase trust in the global technology supply chain. As the forum director, she's responsible for the development of the forum deliverables and for facilitating a consensus on its outreach in harmonization activities. She's been managing customer supplier forums in collaborate development projects for 20 years, and this month the Open Group released its latest standard on combatting counterfeit products.

So, I'm going to start with Jon. You are leading the effort at NIST to develop integrated management systems and standards for supply chain assurance. What types of tools or standards do you think would be most helpful to improving the supply chain?

MR. BOYENS: I think you have to take a look at the different types of standards that are being developed -- or guidelines. What we're doing at NIST right now is really developing guidance for federal departments and agencies, which is going to be from a different perspective than some of the industry-led standards work in ISO and the Open Group and elsewhere.

So, the way we're looking at it from a federal government perspective is through a very holistic enterprise risk approach going from the top organization, looking at the policies down into the program level, down all the way throughout the operational level. So, vertically, throughout the organization, there needs to be different practices, as well as we were looking at the full system development life cycle of the products from initiation and development all the way to end of life.

So, I think in the area of practices, it needs to be very holistic, very comprehensive. Now, getting to that end state is challenging, because right now where the discipline is at currently is fairly immature. So, a lot of research continues to be needed to go into that to validate a lot of the thoughts that we're having on practices particularly in the area of, you know, cost; how validative the practices actually work; how feasible they are. A lot of the research needs to go into that as well.

Fundamentally, it's really a people and processes issue. However, there are tools out there that can help that along. So, a lot of the tools I think that are available perhaps are not being utilized. But there are a lot of tools that could also assist in a process, including different collaboration tools and different mapping tools.

MR. WEST: Okay, thank you.

So, Joe, you direct the software and supply chain assurance efforts at DHS. What are the primary foci of your efforts, and what do you think would make the biggest difference?

MR. JARZOMBEK: Okay, we have both the Software Assurance Program as well as the Supply Chain Risk Management program and with that the part that integrates that is the security automation projects that we have. In fact, I'll tell you the majority of our program dollars go to security automation. That's where we bring the common indexing schemes and enumerations that deal with exploitable constructs in software, the malware, the cyber observables, and structure thread indicators.

And I want to share with you why I think that's very important to what we do, because I think, from a perspective of understanding a way of securing a supply chain and really get assurance out of that is that you have to be able to have both processes and products. You have to have a way of being able to understand the credentialing process is very important, but at the end of the day being able to credential

or understand the resiliency or security or integrity of products is also very important.

So, that's what we have. And we spent a lot of the effort on software at first, so some of you may be familiar with the standards that we've had -- CVE and OVAL, the Common Vulnerabilities and Exposures. That's been very important, but those are only the publicly reported, exploited vulnerabilities out there.

What we've found is that even though we're reaching about 56,000 publicly reported vulnerabilities through CVE, the root cause of those is common weakness -- CWE -- and that's one of the ways that you can literally inspect products from a software perspective, but you also have a way of understanding designer architecture flaws as well. There are fewer than 900.

I almost find it entertaining when people stand up in public and say, we've been a victim of another zero day attack. So, you're just publicly admitting that somebody else was more committed than you in finding your exploited weakness, because those were yours. They were always in there. They are discoverable, and we can mitigate those. We actually have the practices for that.

The challenge is there's not always been the connection between the technology risk and the business risk, so we're helping people understand that so long as you have these exploitable flaws or weaknesses in your products or your systems or your networks, it puts your business or your mission at risk. So, that's one of the ways of helping people appreciate the need to go and fix these things in advance.

We understand, from a supply chain issue, that there are a lot of challenges, because there are people making risk decisions on a daily basis that are simply transferrable, and it's the residual risk that goes forward. People are making risk decisions who don't own the risk. You know, you have developers or disabling compiler warning flags. It's not their risk. They pass that risk on. Compiler warning flags are all

about security risk in the software, so we need to be able to help the suppliers understand why we're concerned about that and having ways of inspecting that as well.

We also understand the challenge with counterfeits. From an industry perspective, they don't have a hundred percent chain of custody. So, what do they do to inspect that, to be able to understand that? And, actually, that's one of the things that we're now turning our focus toward: How do you make this scalable so that you can identify and report counterfeits? Because we within the federal government should not be buying counterfeits.

This is not a matter of well, does it have malware in it. While it may have a higher likelihood of having malware in it, we shouldn't be buying counterfeits. It's a binary, yes or no? Is it counterfeit? Then don't buy that. And we haven't been having scalable means to make sure our suppliers aren't checking for that.

So, that's why we're work-shopping that in June through our Software Assurance Working Groups. And a lot of people have been working in this. We're just trying to make it so that it's scalable to be able to do that. And it's through the public/private collaboration that we do through our software assurance forum that I think has been very successful. Jon and I tend to show up to many of the events together. The only individual who's not here is Don Davidson from OSD, who would typically be here as well.

MR. WEST: And we invited him, but he was not able to make this today.

MR. JARZOMBEK: And the point is that within the federal government, we're starting to move forward in this in the same manner. So, we come in with NIST, with DoD, with DHS and GSA. If we're saying the federal government is moving forward in this, we also deal -- from the Department of Homeland Security, we have a responsibility of helping those who run our critical infrastructure. And all of a sudden,

when you start realizing -- people who run critical infrastructure have the same needs that we have. So, this idea that -- oh, you're the federal government, you represent less than 2 percent of our business -- go away, don't bother me with that issue -- I think is fundamentally flawed, because it's not just the federal government. It's also our suppliers who have the same requirements, and it's those who run the critical infrastructure. And when you understand that our critical infrastructure is laden with exploitable flaws, even counterfeits, all of a sudden you realize why the nation's at risk. But we can actually do something about this. But it's just a matter of public will to do that.

MR. WEST: Okay.

So, John, we've heard from two public sector people describing kind of what they're doing in the government sphere. You and Sally are coming from the private sector. What is it that the private sector is doing, and how do you evaluate their efforts today?

MR. LINDQUIST: Well, we have a program of doing a deep analysis of systems, commercially available systems, for the infrastructure to ensure that there is not anything intentionally embedded in it that would put the infrastructure itself at risk. And a lot of this has been in the press lately because of the HPSI and their report and that sort of stuff, and so I thought it might be instructive.

And then I'll describe what we're doing, but to quote from a letter to John Boehner, Nancy Pelosi, Harry Reid, and Mitch McConnell from BSA Software Alliance, Emergency Committee for American Trade, Information Technology Industry Council, Semiconductor Industry Association, Tech America, Technology CEO Council, Telecommunication Industry Association, U.S. Chamber of Commerce, U.S. Council of International Business, and U.S. Information Technology Office -- and they were sending that back after the latest continuing appropriation. Anyhow, what I wanted to quote was

they say that, “Fundamentally, product security is a function of how a product is made, used, and maintained not by whom or where it was made. Geographic-based restrictions run the risk of creating a false sense of security when it comes to advancing our national cyber security interests. At a time when greater global cooperation and collaboration is essential to improve cyber security, geographic-based restrictions in any form risk undermining the advancement of global best practices and standards on cyber security.”

What we are doing, and what we think should be applied much more broadly, is mostly in the infrastructure area and in the control systems area more than the common IT applications. But take the conversation out of this kind of amorphous, emotional basis and base the whole conversation on evidence; review the product, starting with the source code, starting at the very basic -- and make sure that it is coded in a way that it does not make it easy were it to contain anything that was put there intentionally to subvert the security of the system. And that includes doing a static evaluation of the code, then doing a dynamic evaluation of the compiled code, then running, looking very hard at the hardware to make sure there’s nothing embedded in the hardware that’s bad, then testing the whole system.

Everywhere along the way you do find enumerable errors and problems and things -- you know, everything from hardwired backdoors that were there accidentally, hardwired passwords, inclusion of default passwords. I man, there’s -- and this is just -- these things all exist there, we have been convinced -- at least everything we’ve found is there as a result of sloppy coding, not intentional bad practice, not somebody trying to do something.

But, anyhow -- so basically, make sure the code is clean; make sure the system is clean; then devise a method of making sure that what was clean is what’s delivered to the consumer of the product, whatever it is, because it’s very easy -- and this

is one of the weaknesses in any of the certification things and one of the weaknesses in relying on vetting on people and so on.

If we're looking at well-organized malicious actors, they can subvert any system that anybody wants to subvert. I mean -- and they can certainly subvert any self-certification process. You know, it just isn't useful -- it's much more useful and the higher the risk the more useful it is, and by the higher the risk, the less we would like the consequences of the bad event, the key thing in that risk. But the higher the risk, the more advisable it becomes to actually look at the system, do a very deep investigation of it, and then make sure that that's what's delivered. Then manage this through the life cycle of the system so that as new threats emerge there is a new review of the system just pertaining to those threats, that every time a patch comes out to something, that patch is reviewed to make sure there isn't something in it, because there are -- when trying to insert -- you know, when an organized entity is trying to insert malware, there are lots and lots of different ways to do it that just certifying the organization that developed the system will not protect against.

And the other thing is, too, getting back to the geography of it, I think, as we all know, there's very little -- regardless of whose brand is stamped on it, there's very little that's manufactured in the United States, and almost everybody who has a major or most of the major vendors have very significant operations in countries other than the United States and countries that are not particularly friendly to the United States nor are we particularly friendly to them. And so there are all kinds of opportunities, I mean, to insert things and insert them into a process, you know, subversively into a process that's been all vetted and so on.

So, you know, we think you ought to start from the beginning, review it all the way through, make sure that what you reviewed is what's delivered, and then

manage it through it the life cycle. And that's probably the best way to protect the important -- particularly the infrastructure thing. But I do believe that you could scale that to almost anything if it was acceptable. So.

MR. WEST: Okay.

So, Sally, you direct the Open Group Trusted Technology Forum, and your organization just a week or so ago put out a new standard on mitigating the risk of tainted and counterfeit products. So, can you describe what you're doing and how you believe that helps us secure the supply chain?

MS. LONG: Yes. Thank you, Darrell, and thank you and the Brookings Institute for allowing me to be on this panel with such distinguished individuals who've I've watched on panels many, many years, and I feel honored to be up here with them.

MR. WEST: So, you're humble as well. (Laughter)

MS. LONG: I am humble, too.

MR. WEST: I should have included that in my introduction of you.

MS. LONG: So, yes, the Open Group Trusted Technology Forum did release a standard this past week. It's called the Open Trusted Technology Provider Standard, and it's focused on mitigating maliciously tainted and counterfeit products. It's a set of organizational best practices that when applied -- and they can be applied by component suppliers, providers, and integrators -- when applied will increase the integrity of COTS ICT -- it's focused on COTS ICT -- and help to secure their global supply chains.

So, before I get into a little bit more of the standard and why I think it's valuable, I want to talk to you a little bit about the start of it, which happened about 2009 when the DoD came to the Open Group to conduct a roundtable with DoD and many, many, many mature vendors to talk about the simple problem of how do I identify good, trustworthy COTS ICT? So, they also, in posing that question, said doesn't it make

sense -- this wasn't a directive, it was just a seed -- doesn't it make sense if all of these industry vendors do create quality products -- and in most cases secure products -- doesn't it make sense for them to come together, talk about their good practices, and come out with the best agreed best practices that would become a standard? And doesn't it also make sense, if you're going that route, to create a brand around that so that you can show conformance to that standard and identify trust and technology providers through some type of accreditation program. So, that's how we began back in 2009. Just want to mention this so that you don't think we're sort of jumping on the bandwagon of maliciously and tainted counterfeit stuff, because we've been working on it now for over three years.

So, what the standard does is it really has best practices for all phases of the product life cycle, as John was mentioning, from design all the way through to disposal and throughout the supply chain interfaces. So, we are a global supply -- every vendor has a global supply chain. One of our members says something like everything has a supply chain except for God, and it's very true.

So, part of we're trying to do with this standard is also follow it, as I mentioned, with an accreditation program, and we're starting to pilot that accreditation program where we're working with some of the third-party labs in our membership to create the evidence of conformance and to create the program with us. So, we're piloting that in the next few months and hope to release a public version of it at the end of the year.

And I would also like to say that we're very excited about this first release of the standard, and we think it will go a long way to floating all boats, not just the big, you know, systems providers and vendors but also get to the component suppliers all along the supply chain. But it is version one, so we fully expect that that will become even

more robust after we start raising the votes of all the links in the supply chain. And we're doing a lot of work to harmonize that globally, working with ISO and working with NIST to work through positioning in the cyber security framework, should we be so lucky, and I think by accrediting, having assessment for organizations following these best practices, and demonstrating conformance, that they are following it is a really good step to securing the supply chain. It's just one possible step.

MR. WEST: Joe, you wanted to follow up on that?

MR. JARZOMBEK: I'd just like -- I think it's a great start to be able to do that. There are other standards that will position themselves on system and software assurance, like ISO 1502.6. But credentialing suppliers, I think, is an important step to be able to do that, to be able to assert certain claims about what they're doing.

And we are interested in both tainted and counterfeit products, but understand, when we talk about tainted products, "taint" is in the form of -- it's the potential of having malware or having exploitable weaknesses or vulnerabilities in it. And even if it has the appearance of malware in a product, it does not necessarily mean that the supplier had malicious intent. What we're finding often is it's more about sloppy manufacturing hygiene. They were unaware that their people had downloaded some software from a library -- it could have been a corporate library, an open-source library -- to pull down the functions.

So, again, it comes down to letting the product speak for itself and is there a level of inspection that says I can look for that. Now, there will be some who will say, well, wait a minute; based on that definition of potential malware, exploitable weaknesses or vulnerabilities, means that you could -- every product is subject to being tainted. I'd say, absolutely it is, because -- but it's a matter of fit for use.

A good example -- you know, I live on a lake. It's great for swimming,

boating, swimming. But when I drink that water -- it's the same water, but it's not fit for use. But it could be made fit for use based on how it's treated and everything. So, we want to be able to look at that as far as how do you do that and what are the processes that you do to mitigate the potential risk of taint based on its use?

MS. LONG: Right, and just to follow up on that, Joe. That is why we do have processes and best practices, that an organization can say, I follow these all the time and show conformance to it; I follow these individual products so that it isn't a one-off; here's my product, does it work or doesn't it; does this particular product have any malware in it? But it's -- are you following these best practices all along the way.

MR. WEST: All right, two or three questions I'd like to throw out for everyone on the panel, so whoever wants to jump in can do so.

So, in our opening comments, we've heard lots of actions that are underway in terms of standards, assessment, audits. Sally was just talking about the accreditation pilot they're in the process of developing. The question is what are the primary barriers to making progress in this area? How can we overcome those barriers? And then, in particular, what should be the role of government? Like, some of these efforts that have been described are voluntary actions. Is that sufficient? Do we need a stronger government role in this area? Anyone who wants to jump in. And don't be shy.

John?

MR. LINDQUIST: Well, I think -- and I don't know if very many folks would disagree, but I mean, government for one has to lead by example. So, you know, first things first. We need to get our own house in order in terms of how we handle risk. And that's why we're looking at it from an enterprise risk approach, and that goes all the way from key practices in supply chains, such as, you know, engineering into acquisition and looking at our policies all the way throughout the organization. And that, in terms of

most organizations, is where you have to start, because that is really -- when you're talking supply chain, that is where you have your control -- is in your own organization before you actually try to start putting emphasis or requirements on either the integrator or the supplier that is providing you systems and services -- is really understanding what your own risk profile is before -- I mean, involved in that.

What we're really dealing with is looking at doing a criticality analysis based off of your mission system and components to be able to narrow that down so that when you actually do a threat analysis and vulnerability analysis it's not so extensive. So, the whole issue is to keep narrowing it down. And that's something -- again, this is a nascent problem that we're trying to solve in terms of supply chain, and, you know, "supply chain" has very broad meanings, but I, you know, want to emphasize that at least when we're looking at a supply chain we're talking about the integrity. It overlaps and involves resilience, security, and quality; but what we're really talking about is that integrity piece. And that's what I think over the last few years we've been dealing with. But I think that's --

MR. LINDQUIST: Yeah --

MR. WEST: Yeah, go ahead.

MR. LINDQUIST: I mean, I agree very much that it is a risk analysis proposition and for a long time have held the belief that a significant part of the problem is, in the private sector, that the risk is not well quantified. In other words, you know, my observation is that in a corporation, certainly a major corporation, you've got to get -- to get significant funding to correct something like a security problem, you have to get it to the risk committee on the board, and they have to quantify it, and then if the risk is quantified at a hundred million and it's a no-brainer to make an argument that you ought to spend 50 million to fix it. But we're not very good as a community -- not just

government but just in the technology community -- at quantifying those risks.

A couple of years ago -- probably four or five years ago -- operational risk started to gain traction, and then it seems to have disappeared. At least from my observation, it's disappeared. An operational risk is the risk to your continued operations, not just the financial risks and liability risks and that sort of stuff. But it didn't get much traction, and so it's very hard to make the arguments for implementing the security measures.

MR. WEST: Joe.

MR. JARZOMBEK: When we started our software assurance initiative, we did this from -- both when I was in OSD but also within DHS we carried this through. Every good initiative you focus on people, process, and technology. But we deliberately put a fourth part on acquisition, because our job was to change the consumer behavior, starting with the federal government. So, we've put out a series of pocket guides that are associated with this. One is on supply chain risk management and due diligence, and questionnaires that you should be using to query your potential suppliers about what they're doing, so we get into details there.

We have another one that has sample contract language that once you decide who you're going to team with or bring in their capabilities and products there are sample terms and conditions that you can use.

But voluntary adoption is only going so far, because if we only wait for the acquisition community to focus on doing that, you have to understand, the acquisition community -- the procurement officers, contracting officers -- are not the risk owners; it is the enterprise owners -- the CIO and the critical infrastructure, the guys who are running that.

So those are the risk owners. So, our recommendation is any contract,

before it goes out, just like it has to have a legal chop where we go through general counsel -- is this good to go? -- we should have a cyber security review of every contract before it goes out, and it should be signed off on by the risk owner that says this represents my need. It's not an acquisition decision if I decide to waive off the risk, because it's not theirs to own.

MR. WEST: Okay, Sallie?

MS. LONG: Yes, so, in terms of government involvement, I think the way our forum typically looks at it is that we would prefer government industry partnerships to create the standards, which in the Open Group there's DoD, CIO, DoDA, T&L, NASA; and we need to move that beyond just U.S. governments because it's supply chain. So, we really do need to have industry/government partnerships not only in the U.S. but elsewhere, because we need to make sure that these practices for securing the supply chain are adopted globally.

In addition, I would just like to say that sometimes when legislation comes out that sort of dictates what the industry should do, sometimes the requirements are up here, and the vendors can't meet that like that. So, what we like to think of ourselves as is really industry/government partnership raising the bar to where we can meet it, because you're getting best practices created by industry who is in the field, who knows operationally what exists, who knows the problems, and getting them to work together to raise the bar.

MR. WEST: So, I'm curious to what extent the panel believes that there are technology solutions that will deal with these problems -- for example, the use of labeling and tracking chips, deployment of identity verification solutions -- versus how much of the problem remains on the operational side -- people and processes, as each of you have referred to. What's the mix of what we should be looking for?

Go ahead.

MR. LINDQUIST: To do it at the end of the day, to be really effective at it, it has got to be automated. You've got to be able to check at the receiving end, and it's got to be something that a reasonably educated, reasonably technically savvy person can use but not something that takes some sort of a scientific expert. You know, one of the things I'm thinking about is the DNA approach to it, and it's very hard. Yeah, you can put the DNA on the chip and then you can pass that DNA later, but the process of doing that is very expensive. If you develop other methods of tagging things and looking at them so that you can just very quickly do a quick scan of it of some sort or another and have a very high probability that it is a good component, whatever it is, it will -- I think that's essential, because you're going to get --

MR. WEST: So, Joe, I know you are putting a lot of efforts into the automation aspects.

MR. JARZOMBEK: Right.

MR. WEST: So, could you describe what you're doing and why you think that's promising?

MR. JARZOMBEK: But also, kind of echoing what John was saying, the fact is there's always going to be a combination of how resilient is the product itself and the user's side of it. However, this idea that says it's the user's fault because they opened up an e-mail to have an attachment or they clicked on that you are (~~inaudible)~~ URL ~~like~~ site, my mother should know better, right? It's like why are we deploying products that allow users who would be required to be technically savvy to understand the risk or that my mother must know how to securely configure her operating system. Really?

You know, this is what it comes to. We've got fundamentally exploitable

products, that the users are always going to be at risk, and we can't expect them to do that. However, more sophisticated enterprises -- they know how to do this. But, again, do they have the level of expertise to inspect products before they actually put it into operational use? So, that's where we want to focus on the supply chain side to make it scalable, to turn to organizations who said what did you check in terms of exploitable weaknesses that I care about? These CWEs, these are the ones based on that technology. Here's the top priority. Did you check for these? What evidence did you have for that? That's a great start to be able to -- we want to be able to check for counterfeits, making sure that we're not deploying that.

So, the standards are focused on being able to articulate the things that we care about. You develop the ontology, the taxonomy. We have -- you know, what is it that you're looking for? We have now tool vendors who are in that space who said, I can take that, leverage it so you can automate it; you make it scalable to be able to do that. Static code analysis. We've got pentesting. These are all methods we have today just for software and software enable capabilities, and we're getting better. Just in the state-of-the-art for static code analysis is getting better. There is no übertool. This is a case where you have to bring in multiple tools, and it's making sure you have the right toolkit to bring in those based on the things that you care about. So, we can articulate those in terms of these weaknesses. We can do that in the cyber observables.

At the end of the day we spent a lot of effort focused on malware, because, well, it's just happening. And it's morphing itself, and the threat is constantly changing. But at the end of the day they're going after known exploitable weaknesses and software. It's, why don't you focus on the things that we can control? You can't control the threat. You can understand it, and it's very important that we share information about that because we have such a fundamentally flawed infrastructure that

everybody's got it, so we want to share that information. But if we focus on getting rid of the exploitable weaknesses and making more resilient products, all the bad stuff can be going on. They're not going to be getting after you.

MR. WEST: Sally, what's your reaction?

MS. LONG: So, I would say I think that it is important in the detection of both malware and counterfeit before it gets to the customer. I mean, that's what the supply chain is. And if we achieve that, that's huge. In addition, there does have to be better detection stuff on the other side in case you didn't get everything, because you're not going to get everything. So, I would say it's just a combination -- as we've been saying, it's a combination of many, many different approaches to making sure you're attacking it from all aspects.

MR. WEST: And Jon Boyens.

MR. BOYENS: I think that there are many ways of approaching it. I guess what I'm seeing is there's often a want to try to reinvent the wheel as opposed to adapting the systems that are already there. So, I agree, automation is key in this area. But there are also systems that are already being looked at, such as quality. When you look at an organization, quite often they'll have a different quality stream throughout their organization versus the security stream. So, if you can build off some of the work that's already going on in quality and look at it from more of an integrity perspective, utilizing what is already existing, you can already build off of what is there, and that goes from the testing site as well. Quite often government entities will have a quality side versus a security side. And being able to -- from my perspective, part of that quality is the integrity. So, also building from that, from my perspective, intention is irrelevant. Whether it's unintentional or intentional, it's hard to tell what the intent of the threat is, so it doesn't matter. So, the quality is key. So, it's building off of what already is there.

MR. WEST: Sally.

MS. LONG: I'd just like to go on record. I agree with Jon. (Laughter) Very well put.

MR. WEST: How much sharing of best practices is there across national boundaries, like, U.S. and Canada, U.S. and U.K., U.S. and other places?

MR. BOYENS: Well, first of all, that is -- there's been established relationships among the countries both within the defense side of the House, the intel side. Within the Department of Homeland Security we also have the sharing agreements where we have that. And that's been very important in establishing those relationships to be able to do that.

One of the things within industry -- we've also set up sharing arrangements to be able to do this. Those who are responsible for running our critical infrastructure and supplying to that, there are sharing arrangements already set up to do this. And I will tell you the federal government is sharing a lot of information that goes out, just because individuals -- you don't necessarily see that. You've got to understand, this is (inaudible) to see this. I mean, it would be like somebody who works at a hospital and says, you know, I just want to be able to look at all the patients' records. Well, you don't have a need to know. So, it's based on who has a need to know certain things and types of information you share.

But what we've tried to do is make it so that the sharing of information is relevant so that people can act on it, and that makes the timeliness very important. So, the fact that if you have to have people who have an analysis done before you choose to share things, that's not scalable in a timely manner. So, what we've done, one of the standards that we have -- it's called a structured threat information exchange. STIX is a way of identifying the observable thing -- it's built on CybOX, the cyber observables --

that says I have established a sharing relationship with various organizations and therefore you get to see this kind of information and you get to see this kind. And so as you see things come in, based on the policies you have in place, it's all based on rules. This comes in, it automatically goes out. It's at wire speed now. That's where it makes something so it's actionable. And we've put that in place, and it's now been in place for a few months, the wire speed capabilities of doing that. Financial sector is one of the ones that picked up on it right away. They wanted to adopt these standards.

All right, I will tell you, if you want to look more into any of these standards, if you just remember Making Security Measurable, it's a minor website. They're the technical lead for these various security automation standards. And it shows a relationship. They're all XML based. So, anyone who's got tools -- and you don't even have to make it natively a part of this. You can incorporate that. The transforms are there. So, we're wanting to automate that in order to truly make this scalable.

MR. WEST: Okay.

Why don't we open the floor to questions and comments from the audience? So, if you can raise your hand and give us your name and your organization.

Richard. And there's a microphone coming over to you.

MR. LEMPERT: Rick Lempert. I'm a visiting scholar here at Brookings.

You all have focused on, you know, one really important aspect of the global supply chain, which is the IT aspect, but of course it includes much more. And just to name a few things that I think are of concern, I wonder -- counterfeits ranging from things like drugs, which can be life threatening, to Ray-Ban sunglasses. Another issue is the smuggling of weapons, drugs within the supply chain. A third is disease vectors such as mosquitos in tires, blood diamonds. And, you know, one could go on. Could you comment on steps to protect these aspects of the supply chain? To what extent the

kinds of you do with IT. Things that carry over. To what extent are different things necessary in being done?

MR. JARZOMBEK: We do -- it's -- I will tell you, even from customs and border protection that you've got people, agents, out at the other ends. The Food and Drug Administration has people out at the supply points, the origin of points to do that. They literally have devices now (~~inaudible)~~ in the pharmaceuticals, and it goes from packaging to -- in other words, they already know what to look for, but the reason you have to have devices -- it's about making it scalable. You can't just have eyes on everything to be able to do that.

There are many things that the suppliers have done also to make sure that counterfeits ~~(inaudible)~~ aren't there by saying this is how you would recognize authentic products and that some of that is as simple as the packaging that goes with the hash codes that go with that. For software we have software IDs, the SQUIDs. It's an ISO standard.

There are multiple things that the vendors can do if they feel that that's important. And I will tell you that most vendors understand that when they've got very popular products, all of a sudden they're subject to counterfeiting, they're incented to do this, because, number one, they lose the sale on our side but they also have the risk of brand reputation.

But here's the big however. You can go into any major city in the United States and go on streets and see some really cheap goods that you know are knockoffs. The consumers know that they are. And they tend to have an appetite for that. So, as long -- it's just like with drugs, all these other counterfeits -- as long as we've got the consumer side that's anxious to go take on counterfeits, it's a challenge to do that. There's going to be a market for it.

MR. LINDQUIST: My observation is that it's really difficult to do. The closest thing in the other areas (~~inaudible)~~ on my team is several years ago, updated the International Ship and Port Security Code, and it was a very ambitious scheme where we were going to certify ports overseas and make sure that everything was safe before it left and then if the cargo didn't come from one of those ports it would be embargoed until it was inspected and so on. And it was very ambitious and to the best of my knowledge never really implemented. There were two sets of inspections for the foreign ports, and the first was a preliminary -- or audit, not inspection, an audit of foreign ports, and the preliminary audits were done, and the final audits were never done, and the embargoes never happened, because as we all know the merge on a ship is hugely expensive and you can't just park them off the port and that sort of stuff.

So, trying to do something at the far end, you know, before it's actually received here -- from my observation anyhow -- is, at best, very, very difficult and requires all this international cooperation. And regardless of how much we might want to --

MR. JARZOMBEK: But even shipping companies are positioned to be able to do things that UPS, FedEx -- they're able -- if they were armed with the things ~~(inaudible)~~ looking for these, they won't ship it. So, that's -- there is that level of cooperation.

MR. LINDQUIST: Yeah.

MR. BOYENS: So, you'll see in the different industries that have the biggest risk, right? So, there's one thing to buying a counterfeit purse versus buying a counterfeit bullet-proof vest, right? Are you really going to want to buy a $10 counterfeit bullet-proof vest? Well, it's the same as buying a $3 router off of eBay. I mean, you're getting a good price, but you're inheriting that risk, and you'll -- I think one thing that we

need to do in the IT community is build off of a lot of the work that has already been done in other industries in this area that have been working in this area for the last 10 or 15 years -- the pharmaceuticals, the medical devices. I mean, they have a lot of tools and technologies that they have already been doing and continue to research, that we need to build off of that and start a beginning from a new ~~(inaudible)~~.

MR. WEST: Okay, other questions? Allan.

MR. FRIEDMAN: Allan Friedman. I'm a Fellow here at Brookings. And this is a fascinating panel.

I was wonder if we could open up the discussion to talk about the international aspect. I know we've talked a little about the role of government mandates, particularly for critical infrastructure. And this is not something the United States alone is thinking about. Different countries in the E.U. released report that said, okay, well, this is a risk and what are the different options we have on the table? China and India have a policy of their own. How much do you see this as an issue where there are going to be the large international standards -- will find something other than ISO 27000 that actually works, and how much of this do you see as the potential for an international balkanization where different governments will have different regulatory approaches that could affect the ICD supply chain?

MR. JARZOMBEK: You already touched on that with that, so that was a concern, but I would echo that, say, simply focusing on origin, location is not going to do anything for assurance. You can have just as poorly developed things here in the United States -- you know, poor manufacturing, hygiene; you can have malicious insiders. All of that's there. There will be some people who say, well, there are certain points of origin that represent more of a risk. I'm not going to refute that one way or the other. I will say anything that we do requires some risk mitigation strategy on the

consumer side and from the enterprise. So, what did we check independent -- and let's think about open source. A lot of people say, well, I don't even know where that came from. And so it should be to the point that let the product speaks for itself. It's amazing how many proprietary products actually have open source components in it anyway. So, you ought --

MR. BOYENS: But you know about it.

MR. JARZOMBEK: You ought to get away from this idea that says origin is important. So, the idea of providence and pedigree only factors in, because it's like I don't know how this stuff behaves so I'm going to turn to somebody who I think know, so I trust you, so I'll buy from you. But how did you really know? Do they have fundamental capabilities of delivering secure products and services?

So, that's why we want to look at process and have ways of understanding product integrity resilience.

MR. WEST: Sally?

MS. LONG: Yeah, I'd echo what Joe said, but also I'd like to say that all of the supply chain is working with each other, right? I mean, vendors are buying from -- I think your report mentioned how many different countries are providing components to U.S. providers, right? So, you can't -- I think that "don't buy from here" is a stopgap, and I think it might be a detrimental stopgap, and I think, you know, coming from where I am, working with countries to get them to have their providers adopt the LTTPS best practices all around the globe would be a very important and effective step.

MR. WEST: John.

MR. LINDQUIST: It's a very difficult question. It depends on -- to me, anyway -- it depends on which threat you're looking at. The more pervasive the general threats, the general quality, and so on, there is, it seems to me, a great deal of motion

toward the use of international standards and kind of leveling everything, but if you're looking at the very specific threats and nation states or threats to other nation states, all the standards in the world are probably not going to help on this, because are very actively subverting those standards. So, it depends.

And then you have the other problem. What came to mind immediately was the common criteria and what's happened with it. You know, it started off, and however many of us it was signed up to it, you know, we were going to verify the security of all these things and have all these security profiles, which didn't materialize, and now as a practical matter, at any rate, the U.S. seems to have backed away from common criteria very significantly, not that I disagree with that, because I'm not sure it's particularly useful.

But just as an example of the difficulties of getting all the -- well, one, just the pure difficulty of getting international standards recognized. I mean, that's a long and very difficult process. But then getting people to adhere to them generally is also a very difficult thing and will certainly not protect against the most malicious of the actors out there.

MR. BOYENS: I mean, you -- it's a very complicated -- your question is very general, has many nuances, very complicated. I agree: the international standards are key. But what you're fundamentally asking really involves what you're looking at.

So, that's where I get in to that criticality analysis. You can't make just a blanket statement that you're going to apply this standard across the board for everything. It needs to be a layered approach so that you try to find your most critical systems, your most critical components, and what you do with that. And the threat analysis and the vulnerability analysis, when you get down to those absolutely critical components, is different than how you're going to treat the less critical components,

right?

So, you can apply international standards for the less critical components, but perhaps when you get down to those things that are going to make or break your mission, you're going to want to do extra supply chain research on not only the origin, because again the origin doesn't necessarily matter, but it's what actually has the ability to touch those components and those processes throughout the supply chain. And whatever, whether it's nation state actors, whether it's criminal elements, you want to know the vulnerabilities and the ability for them to touch that specific component. But you can't do it for the entire system. It's too expensive. So, you really need to hone in on the most critical elements.

MR. WEST: So, several of you have mentioned how complicated and difficult it is to reach agreement on international standards. So I'm just wondering, if we kind of look forward 5 and 10 years from now, are we going to end up kind of working through those and ending up in a situation where there are international standards, or are we going to end up in the situation Allan was alluding to, which is a balkanized world where we basically can't figure it out, can't do the international standards, and every country is going to have its own?

MR. JARZOMBEK: I think the international communities where we -- it's a global economy. We have to be able to turn to those. ITU-T has actually adopted our security automation standards under the CYBEX series. So, that's 109 nations that have signed off on that. And it's the use of these standards that we are able to do that. ISO's been very important to that, to be able to do that.

But here's the challenge point. Just because you have a standard -- you mentioned the 27,000 series out there. Great. And they're evolving. They're taking on supply chain risk management type of activities as far as adding to the portfolio of

standards they have. But if we on the consumer side don't even say that that's an important standard, that we're going to buy independent of what you follow, we're kind of sending a message there, aren't we? So, we need to be able to step up the game and expect something that says what do you do to credential your process and your products?

Understanding that suppliers are typically not going to have a hundred percent chain of custody, you brought in things, you cobbled them together, what did you do to expect those to understand that you're not passing on residual risk to me? And that's where there's a promise of things like credentialing. What the Open Group is doing I think is important to be able to do that, because they would checks in there, again, because they don't control everything.

MR. BOYENS: And it's that layered trust, right? So, you can have -- the way we look at it, the utilization of the standard is one thing; the actual conform the assessment is really where you layer on that assurance from self-assessment from third party to third-party validation, third-party certification, post-market surveillance. There are all sorts of conform the assessments that you can layer on top of there to receive greater assurance. But, again, the more you layer on there, the adoption and use of the standard usually isn't where the expense is. It's when you try to provide that evidence in the form of conform to the assessment, which is really where the expense comes from, from an organization, so you have to make sure that what you're requiring that conform to the assessment for is what is the most important.

MR. JARZOMBEK: And understand, there are some people who will actually assert that, well, standards hold them back; it stifles innovation and creativity. I said we ought to -- basically, we build upon standardization. You shouldn't have to be reinventing all of that. Your innovation is on top of standardized ways of doing business,

as well as product integrity.

MS. LONG: Yeah, so, just to add on to what everyone has said, I think assessment is critical, and I think also having a standard and a conformance program that is recognized around the world is critical, particularly for supply chain. And ISO has, in fact -- 2703.6 has reserved a part for this standard either for mapping or for past submission that we're looking at and seriously considering. So, yeah, international recognition, implementing the standard, and conforming to it and that being shown through assessment I think are all very important.

MR. WEST: So, Sally, earlier you mentioned that the Open Group is in the pilot phase of an accreditation program. So, I know it's still in the development phase, but can you just tell us a little bit about how that's going to operate and what you're hoping to do?

MS. LONG: Yeah. So, because it is in development I can't reveal a lot of it, but I would say that we will, in all likelihood, be utilizing third-party labs. They are working with us within the forum to create the accreditation program, and the accreditation program will likely be -- I don't want to say flexible enough, because everyone's, you know, spine will go up, but flexible enough that the applicant can pick their scope of accreditation. So, if they wanted to a product, if they wanted to do a function in a business unit, organization unit, so that we can start focusing on the component suppliers who might want to just one little thing and get accredited for that, and then we move on to bigger organizations who might want to do their whole thing because they claim they use the same best practices throughout. And there will be evidence of conformance supplied, and the third-party assessors will look at that conformance evidence to see if they believe that they have met the standard.

MR. WEST: Okay.

Other questions. Oh, in the very back, what's your question?

MR. DAY: James Day, retired.

Multinational corporations, of course, are always worried about embarrassment factors with the operating groups or subgroups in foreign countries. In the last year, of course, between the *New York Times* and (inaudible), their focus on the embarrassment factor associated with supply chain operations of large companies. I noticed that Darrell didn't include this in his list of eight possible things that can go wrong in global supply chains, and I was wondering: are there any comments or any particular reason why you didn't list the embarrassment or humiliation factors associated with not being able to control your supply chain?

MR. WEST: There are lots of other things that I did not include in the report, because the risks to supply chain are endless, so I tried to focus more on the ICT issue. But, certainly, there have been well-publicized problems in the *New York Times* series and otherwise, and that's a very serious issue.

Other questions or comments.

So, one of the things that a few of you mentioned earlier was the scalability issue. And we know that there are promising solutions that are being piloted in various organizations and in various sectors. The problem, of course, is which of them are going to be scalable.

Of the ones that you're familiar with, what are the types of solutions that you think do have the potential to meet that scalability?

MR. BOYENS: Regardless of what John thought about the common criteria -- and I will agree with him, it didn't meet the goals of what we were trying to do, because, understand, at the lowest levels you didn't even have to inspect the software to assert that you were EAL2. It's -- well, how useful is that?

What I liked about the common criteria was the multilateral recognition.

MR. LINDQUIST: Yeah.

MR. JARZOMBEK: That once you had it tested somewhere, there was a lab that was associated under the scheme that it would be recognized by other countries. So, the idea that if you've got an international accreditation either through 27,000 if comes through the Open Group or other aspects of that, if you can acknowledge that credentialing, both of process but of products as well, those are the two aspects that will make this scalable, because you don't want to have every customer have to go in and inspect both the way you do business and what the product did on its own.

Even within the federal government, you don't have agencies who can do that. There are organizations out there who (~~inaudible)~~ are standing up capabilities that are doing this today where they'll do that for sectors or for some consortium. They will inspect products and let all of their customers know we've done this. And it's against, like, what we have with the Common Weakness Enumeration. That's one of the ways that they'll do that. Even with proprietary products.

So, that's the way that it's going to be able to do it. So, the standardization part of this is important scalability.

MR. WEST: John, your reaction to that.

MR. LINDQUIST: Yeah. On the security side, I think if -- all the solutions are very scalable if the demand exists. They're not if we're going to rely on just government-mandated programs to be subjected to this. But, you know, if everybody demanded that Microsoft products were subjected to some sort of thing before they bought them, then the cost of it although maybe would be very large on a one-off basis, when you look at the numbers of their products that they sell, if everybody was demanding it, then it would probably be pennies per product.

That also applies generally, from my experience anyhow, my observation, to the infrastructures. You know, there aren't that many manufacturers of infrastructure systems, and particularly, you know, were very focused currently in my organization on the telecoms. There aren't that many manufacturers. It's expensive if only one telecomm is looking at doing deep evaluations of it. But if a system is being carefully evaluated and all telecoms were demanding that that be done, then again it scales very nicely and, you know, in some cases it costs millions to do it. When you have procurements that are in the billions, you know, percentagewise it's not very big. So, I think the scalability is really demand based. You know, if everybody demanded it, then it would be able to scale.

I think on the counter-counterfeit side, there are tremendous opportunities for automation things and making them very scalable very quickly -- you know, tagging things various ways and being able to read them and so on; and the devices to read, to identify an electronic component are not particularly expensive. They don't require somebody particularly -- a particular expert to do --

But on both sides I think it is very scalable. I do think that, particularly on the security side, it has to be that it's demanded, though, before it will scale.

MR. WEST: Mm-hmm.

MR. BOYENS: And I do agree with everybody that I think the standards provide that scalability. It's just that right now we're kind of in that VHS/Beta/Blu-Ray/DVD phase where there are a lot of different standards activities in this area, and it's the market that is ultimately going to decide. I mean, this isn't new in supply chain; this has happened throughout the years and standardization, and it's just the phase that we're going through. Five years from now I don't predict that we will be having this same conversation.

MR. WEST: What would that conversation look like? (Laughter)

MR. BOYENS: Well, I think we're going to have all sorts of different issues. But, I mean, the way that we're looking at it from NIST is, you know, if you look at our special publication 853, the new rev. 4 that is out, you'll see five areas that it is addressing. Supply chain is one of them. And why? Because supply chain has been called out as a gap area. So, right now we're looking at supply chain as a gap area that has not been addressed yet, for many different reasons. Well, five years from now, hopefully supply chain practices will be incorporated in everyday business security practices within organizations and we won't be calling it out as a separate issue.

MR. WEST: Okay. I like your optimism.

MR. BOYENS: Well, it's important that we have standards, because when things go wrong people just say, well, I was following best practices. But what are those? Well, the best practices are what are articulated in the standards, and so if they're relevant standards to the product or the domain that a supplier is in, they're going to have to show some level of conformance to those standards, not just say, oh, we do best practices, because they're now going to have to do that. So, that's how they play out. But that's over time. They're voluntary at first, and then after a while it's actually starting to be used in litigation, because it says people are put at risk because you weren't following practices that are universally accepted and will at least internationally accept it, that you've got to show that you stepped up your game.

MR. WEST: Okay, Sally, we're going to give you the closing remarks, then we're going to bring up our second panel.

MS. LONG: Oh -- closing remarks? (Laughter)

MR. WEST: So, it has to be really good here. (Laughter)

MS. LONG: Oh, geez, I didn't prepare anything.

So, closing remarks -- I think this is a huge issue for the world, and I think that we are coming at it at different perspectives, and I think the standards are critical. I think assessment is critical. And I think working together to harmonize those so that we end up with a convergence or even a mapping so that our dear providers don't have to satisfy the U.S. requirements, satisfy Germany, satisfy China, satisfy Taiwan -- the list goes on. And it's also important that we keep realizing that this is a global issue and that we do need to involve everyone in the supply chain if we're going to make a difference.

MR. WEST: Any other closing thoughts from anyone else?

MR. BOYENS: I do, building off that optimism. I would just point out that we're sitting today in a place that we've never been in terms of our reliance upon technology, the vast globalization of economies. So, I mean, between the complexities and our dependence on information technologies and communications plus the globalization that the manufacturing and everything else has, has led us to this problem, which I don't -- it is an issue, but I don't think it's an issue that we can't overcome. It's in terms of building it and looking at it from a risk management proposition like we have with many other challenges.

MR. WEST: Okay.

So, I want to thank John, Joe, Jon, and Sally for sharing their views with us, and we'll move right into our next panel. So, thank you.

MS. LONG: Thank you.

(Recess)

MR. WEST: So our second panel is going to address ways to build trust in the supply chain. So we have Sandy Boyson, who's the director of the Supply Chain

Management Center at the Smith School of Business at the University of Maryland. Previously he served as CIO of the Smith School. And he's also been a technology advisor to the Department of Defense, the World Bank, and other organizations.

For the last three years, he's been acting as a research advisor to the National Institute of Standards and Technology in the area of cyber supply chain risk management. He's the author of several books and articles on different aspects of risk management, IT management, and supply chain issues.

Edna Conway serves as Cisco's chief security strategist for the company's global supply chain. In that capacity, she leads the company strategy to assess, monitor, and improve the security of its global value chain. She also leads Cisco's supply chain cyber protection plan and serves on the company's Cyber Security Board and its Risk and Resiliency Operating Committee. She serves as vice chair of the Open Group Trust and Technology Forum. We've heard from Sally talking a little bit about that. And she also manages the team representing Cisco at the Electronics Industry Citizenship Coalition. Pamela Passman is the founding president and CEO of the Center for Responsible Enterprise and Trade. That is a non-profit organization that develops tools to encourage compliance along various aspects of the global supply chain. In particular, the group focuses on intellectual property and corruption prevention.

Previously she was corporate vice president and deputy general counsel at the Microsoft Corporation, where she led the company's regulatory compliance work across a number of software and service issues.

Andy Purdy serves as the chief security officer of Huawei, a position that he's held for about a year. He oversees the company's U.S. cyber security assurance strategy and systems and supports the global security processes developed by the company's business groups.

Prior to joining that firm, he served as the chief cyber security strategist for CSC and provided strategic input on the development and implementation of company procedures. He also has worked at the Department of Homeland Security, and he helped launch its national Cyber Security Division.

So we're going to start with Sandy. So the University of Maryland recently did a survey of IT vendors to the federal government and found that half never used a risk board or other types of mechanisms. And based on that, in a report you suggested that businesses start to develop integrated management tools and use benchmarking in order to track performance. So what types of management tools do you think would be most effective here?

MR. BOYSON: Okay. Perhaps before I address that directly, I just want to provide a little bit of context. You probably know that the Security Exchange Commission, in October, 2011, had a guidance that basically said that cyber risks that are material, meaning they affect 10 percent or more revenue of a company, have to be disclosed. So there's been 2,000 of these disclosures since then, okay.

And when we spoke with them during our research, they emphasized to us something that we found in our objective survey research, which was that there is a great fragmentation in the management of the ICT supply chain.

So despite the standards, despite the attempts to develop a lexigon, a common definition, a set of practices, the actual management of the ICT supply chain is extremely fragmented inside the corporation and with its supply chain partners.

So the CIO has very limited coordination with the chief supply chain officer or with the chief risk officer. And we've seen this in the 290 companies we've looked at. And SEC, in their analysis of the 2,000 disclosures, also saw this, okay. So this fragmentation is, first of all, not uncommon. I do want to say that we've looked at this

for about 25 years, when we started looking at the supply chain 25 years ago, there was no lexigon. There was on common definition of what a supply chain was. And there were no integrated approaches across the organization that brought together the directors of logistics and distribution and demand planning, et cetera, et cetera, procurement, into a single organization, under a single point of control.

And in addition to these deep structural impediments we saw, which are very similar to what we see today inside the organization, to gain strategic control over the extended ICT supply chain; there was a lack of tool sets for the most basic things, like mapping your supply chains.

When we looked at big companies and we looked at medium size companies, they could not map their supply chain. They could not tell you where all the hubs and nodes of this exploding network were and who actually was controlling the handoffs that occurred in this very complex network.

And with the explosion of globalization of IT in the late '90's, early 2000's, we began to see a new concern over this lack of control. And we began to see things like Score, the Supply Chain Operations Reference Model, which is an integrated framework. It's a code of practice. It's assessments tools. It's all of these things that are now used by about 800 major companies world-wide. And I think today we're in a very similar mode where the dispersal of the IT supply chain in places like China and India have really made it very difficult to gain strategic control. And without strategic control, there can be no trust, okay.

How do you trust an organization when it's fragmented internally, when it doesn't know its second tier suppliers, and when it has a very limited visibility into its risk exposures around the world? How do you trust that entity if you're a business partner?

So our work has largely focused on evidence-based research into what I

would call a new managerial common sense, a new common sense for managing cyber supply chains. And so the last iteration of this work, and we started by looking at several hundred companies, and Darrell reported some of the results to you, I don't need to go further into that, but we saw there was a tremendous lack of awareness of and use of integrated risk governance approaches, okay.

In the last phase of research we've done with Jon Boyens and NIST, who have been our partners and sponsors in this research, we wanted to bring together our previous findings into an automated capability maturity model assessment, a prototype that is composed of a few things. One is a strategic readiness index which looks at the degree of structural integration across the supply chain. Do what degree is the collaboration between CIO's, and chief security officers, and risk officers, and VP's of supply chain inside an organization, these kinds of questions. We also wanted to look at practice maturity. And so we used the NIST IR-7622 as the launching point, developed drill down questions for each of the 10 elements of that IR, and we did that in consultation with numerous industry groups, and we did that in consultation with people like insurance companies who were actually trying to pick up the bill on some of the mistakes that industry has been making.

Which, by the way, there's 50 insurers doing cyber security insurance today. But the insurance coverage that they provide is decreasing. And the set-asides and capital companies have to do are increasing as a result, okay. So it's not just what government is mandating, it's what the marketplace is going to mandate on companies to gain control over their own ICT supply chains.

So the practices maturity index we think is very important. And then finally the last thing we did was created a mapping tool, which is still in the prototype stage, a very simply mapping tool. So you can actually go in and put in your cyber

physical hubs and nodes, identify the transaction sets that occur between them, and import information from established vulnerability criteria like CVSS, et cetera, okay.

And so we hope to be able to complete that. We're discussing how we might do that and make it more widely available. We've only field tested this tool with about a half a dozen major telecommunications companies. They liked it. They had some suggestions. And we will be fine tuning that over the next year or so. So that's it.

MR. WEST: Okay. Thank you. So, Edna, you've talked about how it's important to define processes, products, and practices. So which solutions offer the most promise, from your standpoint?

MS. CONWAY: Well, that's a great question.

MR. WEST: Thank you.

MS. CONWAY: I'm going to give you the three solutions that will solve world peace and world hunger, too, while I'm sitting here.

MR. WEST: That's what we're looking for.

MS. CONWAY: Thank you. So I think I stand in the optimistic column along with Jon Boyens where I think never before have we been sitting at a time where the opportunity between security growth and economic growth particularly have converged. And I think that's because – and Sandy has heard me before, so sometimes I disagree with Sandy.

So I actually think that we have some interesting challenges. I think the ICT supply chain has long had a robust way of measuring risk. And I think that we started things probably about 15 years ago to really look at it. And I think there are others who need to come up to speed, Sandy. And I think that many of us have been thinking about it for a long time. You heard Darrell mention that I sit on the Risk Resiliency and Operating Committee for Cisco. That is exactly what Sandy was talking

about. It's been around for an extended period of time. And we have lots of brethren who we connect with to give us guidance on that.

So we get out there that I come at this from a very different perspective, which is a perspective of optimism, one. Number two, I think that what we really need to do is drive a comprehensive approach. And what does that really mean? It means doing the right thing in the right node of the supply chain at the right time.

And if you look at any of the papers out there, just to understand, the new jargon is really cradle to cradle. For those of us who have been around for a while, it used to be cradle to grave. But in the era of recycling refurbishment and reutilization, it's now cradle to cradle. I'm working on somebody telling me how I go back to the cradle because I'd like to come back for a second try given what I've learned.

But I do think that the way to think about this is a three dimensional approach. So, what security technology, what physical security practices, and what logical security processes need to be brought to bear in each of the nodes of the supply chain? And when I say that, I'm talking about design develop, plan and order, source, build, test and quality, logistics, utilization, sustainment, and finally end of life. And so for me it's those first two pieces of the three dimensional approach. And the last piece is the sort of six sigma traditional supply chain thinking which is logical security process. And if you begin to take that approach, you will find that there are certain things that become apparent on the floor of what you need to do to drive security in certain nodes of the supply chain, particularly for ICT.

But before you do all that, you need to answer the question, what does security mean. And so let me offer what I've embraced across Cisco, which is to really understand that our customers want a couple of things, because we've dealt with a lot of government partners around the world, and it's really interesting to ask the question, what

do you think your problem is and see whether you get either a blank stare in many cases or two words, but no one could articulate it, so here's how I articulated it.

And I think these are very audacious statements, but there are really only three or four of them, and that's to ensure as a customer that what you've received is what you bought, it's genuine.

The second thing is pure. To go back to what a number of our prior panelists were talking about, quality, that not only is it what you bought, but it works the way you intended it to work. And the next is that it allows you to utilize it in a way that precludes or prevents third parties from observing information that you never intended them to see, whether it's nation, state, or industrial espionage. Or whether it's, in my case, my sending a message to my husband about something that I don't want my 27 year old son to know.

And then the last piece is really understanding that we want to give customers absolute trust that what they purchased can be utilized in a way that it cannot be controlled by a third party that they did not intend to have whole or piecemeal control over that system.

So if you take those four concerns, take them to heart, and then start to think about what you do in each of the nodes of the supply chain and say what security technology, what physical practices, and what logical processes shall I deploy, you at least have a framework to begin to assess what works for you.

And we can talk about – I carefully avoided saying what was the best, by the way, and I'm aware of that. I did it on purpose. But we can talk about some examples of that as other colleagues have an opportunity to continue to weigh in with their insight.

MR. WEST: We'll definitely try and pin you down later on that.

MS. CONWAY: Please do.

MR. WEST: Along with the other panelists. So, Pamela, your organization works with companies to improve the supply chain through online assessment and training programs. So how do you think these activities help to build trust and security?

MS. PASSMAN: Thank you, Darrell. And thank you for inviting me to participate today. Let me just step back for a moment and just explain what we're about and why we think we can help build trust in the supply chain over time.

The CenterforResponsibleEnterpriseandTradecreate.org was started just about 18 months ago with the purpose of helping companies share their leading practices. And I didn't call them best practices, I called them leading practices, on how you can best protect and manage intellectual property in your company, whether it's your intellectual property or using another company's intellectual property.

And also we paired this issue with a distinctly different issue, but there's some relation there with corruption prevention. So we are building tools to help companies engage with their suppliers and their business partners to share these leading practices on how you can avoid counterfeits, how you can avoid using pirated software or other content, you know, ensuring you're using legitimate components and software, how you can avoid trade secret theft.

So these are just key components when you think about – you sort of have to step back and before you can even talk about security I think you need to talk about the business processes that a company has to protect its intellectual property.

You know, this is all premised on we want to enable trade and we want to enable innovation. So how can we as business partners ensure that we're all using these leading practices? And we have developed a maturity matrix on what it means to

be able to manage intellectual property appropriately.

We've developed eight process categories and then five levels of maturity. And so we worked with global companies over the past 18 months, probably engaged with about 100 global companies. These are companies headquartered around the world, the U.S., China, Europe, Brazil, Japan that have extensive supply chains.

We also partnered with the conference board and we sponsored a research working group which brought together a number of people from companies who normally don't talk to each other, the chief IP counsel, the chief compliance officer, those people responsible for the supply chain. And we talked through how do you get buy-in from your senior leadership in a company to focus on these two issues with your supply chain? And what are you doing today inside of your company to engage with your supply chain on these issues? And what we learned, which has been confirmed by the first panel and also by Sandy, was that companies are so focused on building the internal processes in their own company that they really have not thought these issues through with their key suppliers. They know they need to, they want to, but it's such a big challenge to take on that they just haven't broken into it yet.

So what we've done is we've designed some tools to help them do that, to help share these leading practices through a self-assessment that's based on maturity matrix that a company will go through and self-assess where they are by answering certain questions. They come out with a rating on their level of maturity.

But we recognize you need some verification, so we have developed an independent evaluation process to go along with this. And we have trained local experts in China and Brazil so far to work with us on this, and the rest is done in English by us, asking a different series of questions that goes to this maturity, as well.

And not surprising, independent evaluators rate the companies lower.

But what's been fascinating to us so far, and we have this being piloted in a number of countries around the world, is there's actually not that much difference between how companies are self-assessing themselves and how the independent evaluators are assessing them.

But what's most important and what we want companies to focus on is what we call the improvement program, continual improvement in maturing your internal systems. So right now in many contexts, vis-à-vis the supply chain, whether it's fair labor, environment, health and safety, you have so many different organizations asking companies, asking suppliers to do self-assessments, questionnaires, audits about the same thing.

And so nobody spends time improving processes. They spend time responding to these questionnaires. So we'd like to get some hopefully traction here where a supplier goes through this create leading practices process once and is able to share it with all of its buyers and focuses and is committed over time to maturing its systems.

We know companies do not want to terminate these key strategic relationships, but they want to be sure that their business partners are focused on continuing to do better, continuing to mature their systems.

So we focus quite a bit on the improvement program. And what was fascinating to us as we started out is there really was not a set of best or leading practices on IP protection. There is in other disciplines, but not in IP. And so the improvement program we have breaks it down for companies on what you need to do step by step in maturing your systems.

We think this is scalable. And we think it's cost effective and it's credible. And we're just starting out. We know the importance of a credential, and so we're

working towards building towards a credential, but that takes time. We hear from companies they want standards. But we also hear from companies they don't want standards. But they want to know what they have to do and they want to know how to do it. So that's the path that we're on to help companies. And we think over time this will build trust in the global supply chain.

MR. WEST: Okay. Thank you. So, Andy, you've indicated that industry-wide standards and best practices are the way to go. Why are you focusing on the industry-wide approach?

MR. PURDY: Well, I think our view is very consistent with what the other speakers on this panel and speakers in the previous panel talked about. For example, Sally Long said the idea of don't buy from here as a stop gap. Joe Jarzombek said we have to get away from the idea that origin is important.

When you look back at some of the detailed work that the Defense Science Board has done over the years, I'm thinking of the microchip study from a number of years ago, the task force that I was on on the mission impact of foreign produced software, the impact on the DOD mission, the idea that it's not a geography base that's the issue. You know, the fact is that we've got incredibly vulnerable networks and systems that the products that go into them are quite vulnerable to begin with. And when you look at the challenge and the risk of a global supply chain, the idea of you need a systematic risk-based approach to address it with standards, with best practices, and I'm certainly quite hopeful that the NIST effort to create the cyber security framework in response to President Obama's executive order is going to help contribute to that, not prescriptive rules, but trying to identify and trying to respond to some of the concerns that the GAO report touched on earlier this month in terms of the need for outcome-based metrics, and the GAO report on standards a year or so ago came out with it.

Although there are a whole bunch of standards in a whole lot of places, the relative lack of consistency with a couple of important exceptions so that a sector knows, not in a prescriptive way, a sector knows these are the standards and best practices that folks need to follow to appropriately mitigate the risk that may apply across sectors, but also within the particular sector.

And hopefully we'll have some time to talk more about the due diligence that was referenced earlier, because I think the issues of due diligence, the question of what do folks need to worry about and what do they need to do about it and are they going to do it. So obviously the cyber security framework effort is going to include an effort to develop incentives. Some of the potential changes that will flow from that in terms of the current sets of regulation under current regulatory authority, that may be revised, and those may impact what unregulated sectors do just as the 800-53 network security provisions that Jon Boyens talked about earlier, that although they apply to the federal government, are being used by a number of different players to basically raise the bar.

And so those questions of things like the pocket guides that Joe Jarzombek talked about, the security profiles, some of the measures and evaluation tools in processes that are out there are things that, if we can build into some of the current regulatory and due diligence requirements such as Sarbanes-Oxley, HIPAA, and Gram-Leach-Bliley without creating a new requirement, but putting some guidance that would help influence folks when they're looking at things like the SEC guidance that came out in October of 2011 as to what is material risk, what are material problems, that can help inform.

So that if you're a C level, if you're board of directors folks, and you're trying to decide, you know, what do we need to do, what do we need to evaluate, and hopefully also go a step beyond that where some of the kinds of things, I think Joe

mentioned contract provisions, to the extent that you can encourage folks, here are some sets of contract provisions that you may want to consider when you're buying from somebody with higher risk systems, I think that can be very helpful. And when you look at things like – and I know the development of the current cyber security framework is not going to necessarily be based entirely on it, but the NIST technical report on supply chain that looked at the due diligence, the roles and responsibilities, the kinds of things that folks need to do from the perspective of not just suppliers, but suppliers are important, but integrators, customers, and network operators, the fact that it really has got to be a holistic risk management approach, and to the extent we can inform it with standards and best practices and guidance and tools that folks should use, frankly, I think sometimes there may be a sense that some of the lessons that folks learn from particular activities that are of significance, of greater significance to higher risk systems such as sometimes common criteria or the dysgenic process, that folks push back and say, okay, well, let's not consider evaluations because it's going to be too hard, it's going to be too expensive, but I think there are some things that we're seeing, you know, Joe said let the product speak for itself, to the extent that we can create an ability to inform customers and network operators and integrators, to give them information, kind of like consumer reports that enables them to say, well, let me make a determinant, here's an easy determination I can make on some level of the assurance of the vulnerabilities in the products, because right now we're at a point that everything is so vulnerable that, you know, we have to move forward to help raise the bar.

And I think the different activities that were mentioned earlier on this panel and the other panel really provide a great deal of confidence that we can really make sure progress.

And I think, in response to your question, although the greatest publicity

and the greatest histrionics tend to be focused on geography or related issues, the kind of discussion on the activities, very active engagement by government and the private sector are the kinds of things that are a very informed nuanced approach that is intelligence and risk-based that I think that, as we work on this together, it's really going to help raise the bar and raise our ability to deal with the risk appropriately.

MR. WEST: Okay. Let me throw out a couple of questions. And again, anyone on the panel can respond. So Andy just mentioned the issue of incentives. And so I'd like to get peoples' thoughts on will incentives work and what kind of incentives have the promise of being effective.

And secondly, I want to go back to a point that Sandy raised initially, which is the question of cyber insurance. Because in other areas, we often deal with risk through insurance, car insurance, fire insurance, property insurance and so on. He mentioned there are 50 insurers working specifically in the cyber area. Is that an approach that would work? So incentives and insurance. What do you think?

MS. CONWAY: So let me take a crack at starting that conversation for us. I think incentives is interesting. It depends on who you're incenting. So for us at Cisco, we're a 100 percent outsourced supply chain. So the reality is in order to embed security concepts into the metrics of how we operate and what we expect of our supplier, there have to be, quite frankly, hopefully more carrots than sticks.

And what that means is, we need to acquire information from some of the leading edge members of our supply chain with regard to some of the unique practices or processes that they're actually either formulating or already well implementing in their own area, whether it's a service or – Alan, you're looking confused.

So, for example, let's say you're working with a semi-conductor provider and they're doing something really unique on segregation of information across the

foundry to make the foundry more secure -- that might be something we'd want to absorb and then deploy across the full spectrum of those semi-conductor suppliers with whom we use. Does that help? Okay. So the reality is, those incentives have to be there with your supply chain partners. Then the question becomes a different one when you start to ask what about incentives for customers to offer to the suppliers to them and those can be different. They could be systems integrators, as well.

And so the reality is, to go back to the point I think that both Andy and Pamela made, is if you have a maturity model or you have a set of international standards that talk about leading practices, what you then empower the acquirer to do is to say tell me not perhaps are you certified to that, but are you engaging in these leading practices, and a certification or an accreditation may be an inpermada (?) of at least third party validation that you are utilizing those, right. So there is sort of that piece that I think is absolutely essential.

The insurance side is a whole another story. And I think it depends on whether you're talking about insuring your own cyber security breaches. But the concept of insurance, to attempt to think about the potential ramifications of a failure of – a scope of ICT products that are broadly deployed across the world, I would love to be the receiver of the premium for that policy.

And so I think that insurance is a very important part of the portfolio of what we need, absolutely. But I think that it can serve as just a piece. And we need to very much make sure we're deploying the right things across that supply chain and have validation methodologies. And Sandy's, you know, reference, quite frankly, to a really robust risk maturity model is another step in that right direction.

MR. WEST: Sandy, Pamela, incentives.

MR. BOYSON: Please.

MS. PASSMAN: When we started our pilot and working through global companies and them contacting their suppliers to use our service, we weren't sure if the suppliers were going to respond. This is something new and different and yet another thing that global companies were asking their supply chains to do.

What's been remarkable is, the suppliers have been very responsive and have very much engaged in the process and have come back to us and really want to engage in the improvement process, which has been the main goal. And they view this as a competitive differentiator.

So, yeah, I agree with Edna, we need more carrots out there. But we also need to leverage the economics of the global supply chain. And, you know, my sense is companies are recognizing that. And we also realize that – we talk about this global supply chain as if it's this amorphous thing, but there is so much interconnections, interrelationships among companies in this global supply chain. So if we can get traction in one of these areas, we really can have a big impact. Meaning many, many companies within a sector share the same companies within the supply chain.

On the topic of insurance, I really hope this is a booming business, because if it is, that means that companies are taking the time to quantify the risk, which they are not doing today. It is just, again, overwhelming. So I hope it's a booming business, if anyone out there wants to get into it. And I hope companies will spend more time quantifying the risk.

MR. WEST: Sandy.

MR. BOYSON: I think a very direct way to create an incentive is, as there's more information about the kinds of provisions that ought to go in the contracts, that suppliers will be held accountable for in terms of whether it's service level agreements or various assurance levels. I think that is a very direct incentive for

suppliers to meet standards.

I'm hoping that the fiduciary responsibilities of the C-level folks of companies and integrators and customers and network operators can be impacted by the cyber security framework. And hopefully the cyber security framework will recommend that part of what due diligence requires is that, for the set of standards that a company chooses, hopefully consistent with whatever the framework looks like, that that company will engage independent third party evaluation of the extent to which they are complying with those standards, and they will provide the results of that independent evaluation to the C-level and board of directors.

I know there's been language in proposed cyber security legislation that that stuff would be made public or whatever. I'll leave that for another day. But if that information comes back with a mitigation plan that's recommended to the C-level and the board, those people will have a fiduciary responsibility to implement that.

And so what we've seen as we've been trying to deal with, and obviously security is a journey, not a destination, as Sandra talked about, the fragmentation of the supply chain. I think what we're learning, I'm sure Cisco is learning as they work hard in this area, is the idea that trying to understand what are the internal security policies and requirements that range from HR to testing to tagging and tracking.

So you do what we've done. And this really emphasizes the audit piece. You have to have separation of duties. So you hold the business unit accountable for implementing the security processes. You have other people within the company, it's their job to independently evaluate whether or not and to what extent the business units are meeting their requirements. And so they identify, and we've seen great results of this, they identify what needs to be done, where the shortcomings are. And it also provides input, a feedback loop which someone mentioned, and a continuous

improvement is critical, so that you can improve your training of particular employees.

So you don't have a business group that's saying, oh, I've got to cut this corner to meet this price. They may try to do that, but you'll have an independent evaluation of what they're doing. You have an independent audit so it can be tracked later.

And then before the product leaves the company, you have another group, independent evaluation of the product, to make sure that you are meeting the requirements. And folks on this panel and otherwise mentioned, and I think Jon Boyens mentioned the integrity idea that we are seeing, and this is a very significant incentive for a company.

We're seeing that because of these independent processes, there's feedback that go into the business group, and the quality of the products become improved. You reduce the vulnerabilities, you reduce the instances of non-compliance with policies, but the quality goes up, because it's much clearer to the business group that somebody cares, somebody is keeping track, and that if also on the end, when the products come out, at least for higher risk systems, if you have abilities in place to have independent evaluations of those products, that, again, provides a feedback loop. And everybody knows you're not going to be able to cut corners. And again, it's a continuous improvement loop. I'm not saying it's perfect. You'll get that feedback that will raise the bar for everything.

And to the extent that we can use these forms of incentive to give greater information to users and potential buyers so that they can compare, like consumer reports for products, you can compare the relative assurance levels, that's going to create an incentive even without regulation, that's going to help raise the bar.

MR. WEST: Sandy, your thoughts on incentives and insurance?

MR. BOYSON: So I think for me the easiest way to look at it is to look at government incentives and market incentives. I think they're different things. So I thing government incentives, when we did our research and a survey of 290 companies, they were different size companies, small, medium, large, and they had different investments that they could make in supply chain risk management and different incentives.

But what universally seem to come out when we asked them the question about code of practice, would they be willing to adapt or adopt a code of practice, we didn't define it too greatly, but what we wanted to kind of get at was sort of what was the trade-off between them doing some things and getting something in return. And the something in return was preferred status potentially for – and contract negotiations because they showed a higher degree of assurance, some potential for relief from liability, okay, associated with the work that they do. And then the other thing really was some relief from regulatory overload, so streamlined relationships with their acquirers, okay. Those were big incentives for the group that we looked at, which really cut across the ~~(inaudible)~~ size spectrum of companies.

Now, if you look at if from the perspective of markets, activist shareholders and Security Exchange Commission and others I think recognize already that cyber is becoming a force and a factor in assuring revenue stability to shareholders.

When we were told, I can't go into detail on this, that one bank had a billion dollars in ordinary, necessary expenses as a write-off associated with cyber breaches, and you can sort of begin to understand how that might not be acceptable to its shareholders and would demand a higher level of accountability by the risk management function of the board, as well as the company.

Now, I also would just conclude by saying that it's kind of old hat in a place like Canada because the Day Report, which goes back well over a decade and a

half, has made it a priority and, in fact, a prerequisite to list on the Toronto Stock Exchange. You've got to have a risk governance structure in place. You've got to show that you're doing risk assessments on an annual basis, that you update them, and that you're making progress toward mitigation of those risks. And you cannot list on an exchange in Toronto unless you show those things.

And so the SEC has made this tentative step toward that kind of recognition, tentative step. But I think ultimately, if they're not going to do it, the exchanges need to look at it. And if the exchanges are not going to look at it, I can tell you the insurance companies are looking at it, okay. They're changing their whole risk models after Thailand and Japan and they're looking, you know, they're looking at the claims that are coming in, okay. And they're basically saying you better do a better job of quantifying your risk exposures if you want to get any kind of insurance coverage with us.

And so premiums is going up, coverage could be going down, and it's creating a situation where, unless you're very, very big and you can form captive insurance companies among – either from your own reserves or in combination with other companies in your industry, it's going to be increasingly harder to transfer risk. That's how I see it.

MS. CONWAY: You piqued my thoughts on something when you said relief from regulation and regulatory overload in particular. So there's something that we can learn as to why – to go back to what I think Andy articulated correctly, at least in my view, which is why those international standards are so important in giving acquirers, if you will, I like the analogy of the consumer reports, but it's going to take public private partnership. And here's the reason why.

Quite some time ago in the ICT community, we saw exactly what Pam said earlier. We're using the vast majority of the same supply chain. And if you were to

walk into a manufacturing facility, what you would see in the sign-in sheet was the list of 20 people from Cisco, 30 people from HP, you know, 15 people from another company. And at the end of the day, you'd look at your folks and say, it's amazing you actually get any product out the door because you all are very busy giving us tours and answering our questions and dealing with audits.

So we put together something called the Electronic Industry Citizenship Coalition where we recognize that if we took our competitive hats off for a moment and we focused on four foundational elements somebody earlier, a gentleman in the back I think who is retired talked a little bit about reputation and brand, and somebody else asked questions about other areas, and in this case it was the ICC focuses on ethics, so it's sustainability, labor, and human rights, and two other categories. What we did was we put together a code of conduct. And we then said we're going to do audits where we all collectively share. So if they're a member of your supply chain, sort of – I think, Pamela, one of the efforts that you're leading, you will get this report, and you get the benefit of it without, you know, all of us being in there at the same time. And it's worked and it's been beautiful. And we've certainly looked at the inside of the Open Group technology partner standard as an example.

Where it breaks is, if you don't have partnership with the public sector. And here's a classic example why. So if you look at what the EU did with European restrictions on hazardous substances, they put together an invaluable effort. We all need to pay attention to it or we won't be worrying about cyber because we won't have a planet to be residing on. So they're removing certain elements from electronics.

What they did do was, and what we didn't do a good job of, was partnering with them and educating them. So they ended up imposing restrictions that, because of the laws of physics, were impossible. So 32 exemptions needed to be

written, recognizing that if you do what was actually asked, the product will not work.

Another example is what you just saw, to go to the SEC. Recently we've seen – everybody is talking at least in ICT about conflict minerals, right. So it's our version, if you will, of blood diamonds, where there are a number, it's tin, tantalum, tungsten and gold. They're mined in a way that is ethically something we do not want to support as a nation, as individuals, and as members of the ICT enterprise community.

However, what we now have is a regulation that says you need to report exactly what you're doing with a recognition that failed to acknowledge that we have to figure out where the ore is mined, and you have to at least go to the smelters and figure out all of that subtlety, and quite frankly, complexity, and some of it is going to be very difficult to do. So again, the ICC has stepped in.

So I think Sandy raised a very interesting point, which is the beauty of this is, if you do it right, you can minimize, I won't say absolutely eliminate regulatory overload, and hopefully develop a partnership where I'm looking at Joe saying, Joe, you know, I believe in ~~(inaudible)~~ static and dynamic and pen testing and that's all cool, but we have some other ideas, let's think about that and let's share it openly.

And how we do it, we all can differentiate. So the beauty of this is, you preserve intellectual property, you create new technology and intellectual property, you protect it under the theories that Pamela is articulating with recognition, and then you blend it into a set of risk analysis that Sandy is talking about, and then you bring it to bear to those who would acquire under the schemes that Andy is talking about. I think I just wove all of us together. But it just came to me that I think we all have pieces that, together, will come pretty close to not perfection, but boy, wouldn't it be great if we could achieve that. And we've done this before. I can't hope but be optimistic about it.

With the talent, the integrity, the enthusiasm, and the degree of work

that's going on, we will achieve this goal. And as Sandy pointed out, if we don't, our insurers will make us.

MR. WEST: It sounds like you've just created the general theory of the supply chain. Congratulations. Andy.

MR. PURDY: Let me follow up with the point that Edna made regarding how you get the product out the door. I think there's a common view, and I think it's, at least in my view, it's a misconception in terms of, okay, security is going to add all these costs, well, what we found is, by the kind of independent evaluation process that we've been talking about, there has become an incentive in a couple ways that directly relate assurance with quality.

So because we want to be able to track where the different components came from within the company and where the components came from sourcing, and we have a feedback loop if there's a problem that helps us improve the process. But also, what it has meant in terms of the business group is, there has become an incentive to create only those variations of products that are necessary. How many different variations of something do you need? When you're a global company, you might say, okay, we'll do this here, we'll do this there, but as you're doing the assurance and these processes, it's required that the business group has to be able to track and we have to be able to evaluate everything that comes out.

And so it's basically saying, okay, what can we have as a core platform and then what is the absolute minimum variation we need to meet a particular region or country or customer need?

So it means you end up with a more efficient business process, a greater focus on let's limit the number of products, let's increase the quality, and let's raise the trust level in the assurance. So that creates a great internal incentive for improvement in

both assurance and security.

MR. WEST: Why don't we open the floor to questions and comments from the audience? So again, if you have a question, just raise your hand; give us your name and your organization. Any questions? Alan?

ALAN: So a number of you talked about the SEC guidelines or suggestions. And, Sandy, you've done a better analysis than I have. I read through them looking for any disclosure that wasn't known publicly to the market. And outside of some fines or settlements that were previously kept sealed, I haven't seen any new information coming from SEC disclosures. How important is transparency, public transparency, not just internal information between suppliers and contractors, to solving this problem? And will we need a sort of stronger push from the SEC or other regulatory guidelines or can this be solved by private information sharing agreements without public knowledge?

MR. BOYSON: I think it's a very good question. Perhaps I'll take the liberty of just sort of commenting on it. Two things. One is that the SEC has not fully analyzed the 2,000 disclosures. They were very clear about that with us. And apparently there is a database available now that people are starting to look at. We have not done that either, okay, because you have to go through them literally one by one, so that is an issue.

But in terms of accountability and transparency, I just want to refer back in sort of the spirit of this is solvable, you know, this is something that people get, you know, we created these supply chains, we can gain control over these supply chains, okay.

This was the same question in the early '90's that the chemical industry had, okay. And so I want to talk just for a second about the Chemical Manufacturer

Association which we work closely in a partnership with, Department of Energy and the Chemical Manufacturer Association, because they have a public private partnership, as Edna talked about. They were the largest HAZMAT shippers, the DOE. And they were very worried, as the industry was, that they would have an accident that would impact hugely their reputation of the industry. So the industry was very interested in working with DOE because they were in the same boat basically from a liability perspective and branding perspective.

So you may have heard of responsible care, okay. I think it's really a model for some of what is being talked about in the IT security industry. First of all, it's a condition of membership. You cannot opt out. If you're going to become a member of the leading industry association, you have to ascribe to the set of quality improvements, okay.

Second, there's a CEO level commitment. They have to declare it in a letter of commitment that they are going to work in this area. So the CEO has to support the security organization or the quality improvement organization. It can't be, you know, just focused on (inaudible).

And there is an evolving definition of what is leading practices. It's changing all the time as we learn more. This is all about learning. And that translates into training and third party trainers and consultants that go out for organizational improvement of companies. And then finally there is third party certifications like what Open Group is describing. And this has been done for decades. And it evolved from the United States. It's now global, it's all over the world, and it's the way that the chemical industry I think has really provided us a potential model in the IT security industry to look at.

MR. WEST: I have a question about work force development. Because

several people have suggested several ideas in terms of audits, independent assessors, third party labs and so on. Where are we going to get the workers for this? I mean it's kind of a new area of expertise. And don't look at me like I'm crazy.

MS. CONWAY: Well, I think a lot of it starts with companies and training their employees. And this is actually some of the feedback we've gotten from the suppliers and manufacturers that are piloting our services, you know, do you have online training that can help our own employees understand, you know, how to protect intellectual property. We're getting a lot of requests about how do you protect trade secrets against theft.

And work force training always does start inside of a company in terms of training people, identifying specific disciplines, how do you build these disciplines over time, what kind of credentials do these individuals need to advance in this discipline. So I think companies starting internally is quite critical. And, you know, organizations (inaudible) create. And we view building a whole training program around what we're doing is a critical part of what we will ultimate deliver to the marketplace. So I think those two combinations.

And, you know, it also starts with government. Government I think is understanding that it also has new disciplines that it needs to have a work force around. And being able to communicate to universities, to community colleges, you know, what are those disciplines, what is the make-up of the kinds of skills and experiences people should have in those disciplines.

MR. WEST: Okay. Other questions or comments? And don't everyone speak at once because that's really rude, you know. Right here. Actually, wait for the microphone to come up just so everybody can hear you. It's coming up right behind you.

SPEAKER: Getting back to the insurance stuff, has the insurance

industry made sufficient advances in their actuarial processes on security, you know, cyber security things to effectively –

MS. CONWAY: Sandy, you better take that one.

MR. BOYSON: Yeah, you know, that's a really tough question. I mean they're meeting on this all the time. I mean I'm sure you know, for example, in the natural disaster arena that they've had constant modifications in the last year and a half of the, I believe it's called the RMI, which is their underlying modeling that they use for impact analysis. But, you know, when you have a $500 million claimant out of Thailand on IT manufacturing, it kind of screws up your modeling if you're an insurance company, you know. So they're going back and revisiting that. That's actually what happened. There was a $500 million claimant out of Thailand.

So my understanding is that that's like the big issue right now for a lot of insurers who want to get into cyber. I mean they don't feel confident that they can analyze the exposures or that the information is readily there to analyze the exposures. And I think that's creating friction.

MR. WEST: Okay. Alan had a follow-up question.

ALAN: If I could offer some thoughts on cyber insurance. So everyone on the panel has talked about that you have to look at it specifically. So some areas, for example, PII protection, we've seen insurance really stepping up because we're able to, even if we can't predict the risks, we can understand the magnitudes of harm. And that insurance market has matured.

In other areas, while it is a fairly common practice, more and more people are entering it. Usually it caps at a pretty low level. And again, outside of financial fraud, where again you can estimate and model, large firms self-insure, small firms don't care, the real risk is at the middle. And if I could just put in a very quick plug

for those of you that are interested. The work shop on the economics security will be in June at Georgetown, if you're interested in learning more.

MR. WEST: Okay. Yes, Rick.

RICK: Most of the discussions focused on sort of intentional subversion or accidental subversion. Darrell's paper has other dimensions such as the Tsunami which can disrupt the parts availability and the like. Can you talk about this dimension of sort of ensuring that physical or other disaster or economic slumps won't interfere with the supply chain?

MR. BOYSON: That's Edna. I think Cisco has done an incredible job, really an incredible job in dealing with the Tsunami. And it's a model. We study it. We teach it to our students. In fact, I just did that for half a day. We just covered Cisco's response to the Tsunami. And I think you should really tell them a little bit about what you've done.

MS. CONWAY: So we have a pretty robust risk and resiliency program in supply chain. Obviously we feed up to the risk and resiliency operating committee. But I think what we've done is, go beyond business continuity planning, which does include the economic factors with a constant measurement. We had the privilege many years ago of having a Stanford mathematician PhD come to the supply chain and build some of the foundational risk alga rhythms for us. And that was Edward Erickson, by the way. So we've moved risk continuity planning into something, if you will, that goes beyond just the sort of traditional, narrow minded supply chain, well, where is their inventory located, et cetera, right, into what are their economic situation, what's the geopolitical situation, what's the reality of the physical geography where they are, and calculating frequency of, you know, hurricanes, earthquakes, et cetera.

And then on top of that, we built, and I'm doing it a disservice because

it's complex, so bear with me as I try to make it general, an incident management playbook that, in all honesty, for all of us, what we found is, it's the reason why I love seeing people with, you know, gray hair, because you learn from having lived through things, right. We can all learn something from those folks who are senior to us and have experienced things.

MR. WEST: I'm glad there is something good that comes out of that.

MS. CONWAY: There's a lot of good that comes out of it. And so what we've done is, build a playbook with a set of steps where we now have an incident management team just for – well, we have one for the company, just for supply chain that brings together instantaneously and hopefully in advance because we are regulatory as part of that continuity business planning. We have methodologies and feelers out there to get information on all of the categories of areas that might cause potential small problem and weak – up to wreak havoc regulatory real time. And, you know, a bunch of us have pagers that, you know, go off when something is happening, and we convene in advance.

But what that incident management team does is analyze comprehensively – remember how I said you have to do everything comprehensively across the entire supply chain? The reality of who's impacted and here's where what Sandy said I think comes to bear, when he did his research, 290 companies couldn't map their supply chain. And his point in that is manifested in an incident management circumstance.

If you haven't mapped your supply chain, and you have a Tsunami hit a site, and you don't know where else you can go to, you have a bigger problem than the Tsunami coming at you, okay.

And so it's almost foundational in this day and age to business continuity,

savvy business continuity, and if you begin to think about circumstances where you put everybody together and what we did was we literally walked the playbook. We hadn't had a Tsunami, that wasn't one of the physical events that had ~~(inaudible)~~ hit us, but actually started to talk about who's doing what, where, what can we move, can we leverage things by, you know, moving things up, down and around, do we need alternate transportation modality, all the things that you sit here and you nod and you say yes, of course you would think about that. But I think Sandy's research proved that, we say of course, it's actually not of course everywhere, right?

MR. BOYSON: That's true.

MS. CONWAY: And so developing that – and part of what I've been doing is, I've had the privilege of leveraging that robust foundation. And so I came in in the Tsunami and said great, we just moved some equipment to the second floor on that same building, lovely, is the access control the same, is it coordinated with the information management system? Oh, by the way, are the guards still outside or are they home sandbagging their homes for their family, which is, by the way, where I would be?

So perhaps we better think about security in the context of this incident, right? Remember, technology, physical, and logical at all times. So I've done it a great disservice. It's far more complicated than that. But it's premised on end to end, every node's expertise sitting at the table, constant algarhythmic refreshing of information unlikelihood of events, and then building on the knowledge of, all right, we've lived through a hurricane, a Tsunami, you know, the volcanic eruption, which I can never say, so we just call it the Icelandic eruption which caused, you know, havoc for lots of us. And slowly, over time, you learn two or three things that get built into the playbook. And you go, all right, something else for us to checklist off of. And that's how you build robust risk management.

But I think, you know, I made light at the beginning that sometimes I disagree with Sandy, but I was joking to some degree because I've got to tell you one thing that he said that's absolutely foundational. Understanding what's going on, where, if you want to deploy a horizontal capability like security or risk management, you can't do it without that foundational mapping, absolutely not.

And when you think about what lies at the heart of, at least for folks like Cisco and some of our brethren, it's intellectual property. So if you discount in any way what Pamela is talking about, you're missing the fact. If you don't understand, A, what your intellectual property is, and you don't understand where it is and how to protect it, that needs to get mapped into that risk plan, as well, from a company perspective.

MR. BOYSON: And the proof is in the pudding. If you look at the sense and respond capabilities that Cisco showed in the Tsunami and you compare it, what we would call ERN plus or enterprise risk management plus, because it's sense and respond, and you look at a traditional ERN system where, you know, every six months you look at, you know, your risks, you know, that kind of thing, it's more of a planning-based activity than a capability-based activity.

Look at Erickson, okay. So as a result of what happened in the Tsunami, Erickson basically had to sell off. And then shortly thereafter, they had to – what happened to Thailand, there are not longer Sony Erickson, okay, it's just Sony now, okay.

They had to get out of the business. They got pushed out of the business because their production collapsed coming out of Japan in terms of mobile phones. And Sony had to literally take over the business. They had to sell out.

So if you look at that, and we looked at what happened with Cisco, they didn't lose a beat. They didn't miss revenue targets. You didn't miss. I mean it's very impressive –

MS. CONWAY: Lots more gray hair, but no revenue targets lost.

MR. BOYSON: Yeah.

MR. WEST: Okay. Other questions? In the back row there's a question.

SPEAKER: James, sorry ~~(inaudible)~~ for Ms. Passman. You talked about your work in increasing greater compliance (inaudible) intellectual property but didn't say too much about prevention of corruption. Could you talk about uniform corruption standards with respect to headquarters and local operations and standards and practices?

MS. PASSMAN: Thank you for that question. What we have seen is that there's actually more of an idea based on a lot of great work that different organizations and companies have done over many years, from Transparency International, to the OECD, to the World Economic Forum. The recent release by the DOJ and the SEC of their guidelines, information and guidelines about the UK and our (inaudible)

There's a good sense of what companies need to do, again, the processes and systems they need to put in place to address corruption prevention. And our engagement with companies, again, very focused internally. It takes a lot of work to implement these processes and systems. Especially in a far flown global company, it takes time. And you need to have a lot of checks in place.

You know, companies recognize they need to extend this to certain key third parties in their supply chain, in the value network. And there again, similar to intellectual property, although the standards are not so well defined, they're struggling with how to do that. And we believe it's a very similar approach, a very similar management systems approach for intellectual property and for anti-corruption. You

know, do you have the policies, procedures, and records in place? Do you have a compliance team in place? What is your risk management process? Very similar sets of processes and systems you have to have in place. And so our service presents both of these, you know, subject matter separate, of course, but a similar way for companies to approach these issues, again, extending it into their key third parties.

SPEKAER: Following up, do you have any recommendations that companies really (inaudible) audit themselves?

MS. PASAMAN: You know, I have become a little sanguine about audits. And I would refer to a book that's coming out very soon by the MIT Professor Rick Locke that's done quite a bit of analysis of, you know, codes of conducts and audits, whether it's company audits or third party audits. And it's been a system that really has not driven systemic change, which has very much influenced the approach we're taking on this, you know, more capacity building, more sharing of leading practices, working on continual improvement, measuring where you are today, and measuring where you can go and your progress over time.

So I'm not the right person to comment on the audit process. But I think – and I would recommend this book because I think it will be very instructive. As we think across these different security related issues, you know, how do you frame the engagement with your key third parties? And it's got to be collaborate, it's got to be long term, it has to be flexible, but it's got to recognize that there's benefits to both parties by maturing and advancing the way that you operate.

MR. WEST: Any other questions? Maybe I can close by coming back to the global aspects of this problem. Because each of you in different ways works across national borders. So I'm just curious. If each of you could share your view in terms of how different countries and different governments are handling this and what the issues

are in terms of cross country aspects of the supply chain.

MS. CONWAY: So I'll make a personal statement and then I'll answer the question. The personal statement is politics has no place in empirically supported security endeavors, period. No ifs, ands, or buts. But I don't live in Candy Land, I live here on Planet Earth. And the reality is that the international cooperation is better than you would think. It has room I think to grow.

I would not make light of common criteria because it is the only place I know where 26 countries have actually looked at one another and said I will mutually recognize something that one of you has done, whether – not all of them – there's participating countries and issuing countries, but it's still a model. It's the reason why other international standards want to harmonize. I think the difficulty is, sometimes security becomes the foil and supply chain in particular for other concerns, whether it's what some of our colleagues very appropriately are concerned about in India in terms of not losing intellectual property and seeing some of what the United States did and being concerned about it and using, quite frankly, security as a way to deal with indigenous innovation.

So I think you have to be open minded and say let's share what we can. But it goes back to international standards as a way, a small set. Give us a language that works across the globe. And it is one where all can participate. Regardless of the fact that it takes a while and it takes some time, it is so worth the effort at the end of the day because you have a common parlance which you can then deploy and everyone begins to understand despite all of the other political overlays.

MR. WEST: Sandy, your thoughts on the global aspect?

MR. BOYSON: It's really tough. It's a really tough question. Okay. I'm chairing a committee, it's called the IT Committee of the Department of Commerce, Supply Chain Advisory Committee, and part of what we're doing in the committee is,

we're looking at EDI and single trade windows around the world, okay, just at that level, okay. And it's just amazing that there is no regional single trade windows that we can see anywhere in the world. So countries have not been able to get out of their box to even have an electronic system for identifying and having common elements of trade. I mean obviously there's standards like edifact and things of that nature. So they haven't gotten out of the box on that one, okay.

And if you look at – even at the TPP, the Tran-Pacific Partnership, which is a free trade agreement, it's the first time, and I know this because we've done some work in this area with the trade office, the Office of Trade, and it's the first time supply chains are even explicitly mentioned in any free trade agreement, okay.

And so the ability of countries to come together and share information and do sort of due diligence together over critical supply chains that operate across borders were just learning how to do that. So how does that translate into the ICT space? I don't know the answer to that.

But I suspect that there's going to be a need for some type of common surveillance, common shared sort of real time understanding of what's threatening the ICT environment globally and we don't have that right now. I'm not talking about standards, I'm talking about something much more immediate.

MR. WEST: Okay. Pamela.

MS. PASSMAN: Well, you know, it was my experience at Microsoft, and certainly in the last year and a half with Create, that companies want to be part of the global supply chain. Those that are in it find great value in it. Those that aren't aspire to be in it. So the approach that Create is taking is really one company at a time.

It's a long process, but, you know, we need courageous multi-national companies to say this is important to us, we're going to engage our supply chain, and we

need companies around the world that are in the supply chain or aspire to be in the supply chain to want to raise the bar on how they operate.

MR. WEST: And, Andy, we'll give you the last word on this.

MR. PURDY: Well, it's a little hard to tell on the outside how much active collaboration and information sharing there is across governments even among the U.S. and its allies in terms of supply chain risk, vulnerabilities, particular kinds of threats. I'm optimistic that the efforts of both the collaboration that's going to lead to the cyber security framework and developments on that over time and the work of the Open Group and the Open Group collaborating with ISO and common criteria and others, I think the pre-eminence of the private sector role in developing standards and the value, the business value that will be obtained as those standards become clearer, so that relationships between customers across borders, there's going to be a tendency to rely on those standards, to audit against those standards, to put contract provisions that hold people accountable for those standards, and I think that will form a very good basis.

I think for higher risk things, I think some of the measures that I expect or think might be implemented by GSA in terms of procurement requirements, I think as those requirements become clear, if they actually do do some of the things that the procurement folks haven't really done over the years, to have some baseline levels of life cycle assurance requirements, I think that's likely to be adopted and followed and perhaps, with input from other countries, be modified that, again, for higher assurance things, I think that's likely to, in effect, be a set of standards that all can aspire to and be held accountable for.

MR. WEST: Okay. We'll make that the last word. But I want to thank Edna, Sandy, Pamela, and Andy for sharing their views with us. We look forward to the continuing efforts at NIST, the Open Group, and DHS. And we appreciate all of you

coming out to join us today. Thank you very much.

* * * * *

CERTIFICATE OF NOTARY PUBLIC

I, Carleton J. Anderson, III do hereby certify that the forgoing electronic file when originally transmitted was reduced to text at my direction; that said transcript is a true record of the proceedings therein referenced; that I am neither counsel for, related to, nor employed by any of the parties to the action in which these proceedings were taken; and, furthermore, that I am neither a relative or employee of any attorney or counsel employed by the parties hereto, nor financially or otherwise interested in the outcome of this action.

Carleton J. Anderson, III

(Signature and Seal on File)

Notary Public in and for the Commonwealth of Virginia

Commission No. 351998

Expires: November 30, 2016