Committee on Homeland Security

Oversight, Investigations & Management Subcommittee

Unofficial Transcript of Chairman McCaul's Exchange with Witnesses

July 7, 2011

McCaul: Mr. Toohey, I want to start with you. We have some photographs I hope we can put up on the screen that deal with the issue you were talking about. This is a semiconductor chip that includes information about date and manufacturing location codes. Is that correct?

Toohey: That is correct, Mr. Chairman.

McCaul: Why is that important?

Toohey: It's important because in this context it enables us to determine whether or not the chip is authentic or counterfeit. Companies have databases which can tell you exactly where the chip was manufactured, on what day, what type of chip that it is. And by verifying the type of chip versus that coding system, we can almost instantaneously verify whether that is an authentic chip or not.

McCaul: So DHS would come to you and say 'hey, we got this chip, is this authentic, is it yours?' And if it's not, if it's counterfeit, they need to confiscate it, correct?

Toohey: Yes sir.

McCaul: That was the practice…

Toohey: That was the practice for many years.

McCaul: 2000-2008 are the years…

Toohey: Even before, Mr. Chairman. Even before 2000 it was the practive for many years. Starting in 2000, they stoped sending us the actual product and just sent us pictures which is fine. As long as we have the code we can determine… It was actually a system that worked very well, but in 2008 it all stopped and they redacted the information from the pictures that they were sending.

McCaul: So, they would send you the actual product, which is the best evidence, and then they would would send you the picture, which had the information on it so you could identify, and then in 2008 something happened… Let's show the other picture [picture shown]. This is what you get. Is this an example of what you currently receive from DHS?

Toohey: Yes, Mr. Chairman. As you can see, it's virtually imposible- you can't see the number, and it's virtually impossible, based on that, for anyone to authenticate that chip.

McCaul: You don't know the trace codes or any of the information contained in the previous photograph to identify this intellectual property, this semiconductor chip?

Toohey: Yes, Mr. Chairman, that's exactly right.

McCaul: It's astounding. Why? Has DHS explained to you why they stopped providing this kind of information?

Toohey: Yes, and let me first of all clarify that this isn't a policy that was directed at only our industry. It affects all products and was based on a reinturpritation at Treasury Department, which has policy responsibilities in this area. Established in 2000, it was a reinterpritation of the Trade Seceret Act, in which it determined that by sending that information to the manufacturer, it would violate the disclosure of financial information provisions of the Trade Seceret Act. As I mentioned in my statement, that just doesn't make any sense—even common sense. To the extent that anyone owns that publically viewable information, it's the manufacturer, it's the companies that it would be sent to. We provided detailed legal analysis to the Department of Treasury and DHS to why that just isn't the case. They haven't really given us any reason why our legal analysis is wrong. Part of the motivation that I understand is a desire to protect parallel importers, so not to have any information disclosed to manufacturers that affect importers. But there's nothing in that code that can tell us who the importer is. At the most, it could tell us who we originally sold it to but that information simply is not possible to obtain from that code. So, from our perspective, that doesn't make much sense. And if one could even understand that justification for handbags or some other products, one could maybe understand it. But for products where there is critical life-saving technologies, health and safety, our soldeirs' technology on the line, we know for a fact- as you said in your opening statement Mr. Chairman- this is a clear and present danger. We know that there's 15% of current inventories of the Pentagon where these chips are counterfeit. We know this is a problem. We know this is an ongoing issue and it is affecting the lives of our soldiers and the health and safety of our citizens. So in this particular area, it just doesn't make any sense to us why we would tie our hands and not allow our industry to help the government determine instantly where these products are coming from.

McCaul: You want to help to help the government identify counterfeit chips and it's my understanding that the lawyers at the Department have now determined that they cannot give you this information unless they have basically taken all of the identifying information off of it. How can you possibly identify if something is counterfeit when they have taken off all the code numbers?

Toohey: You're exactly right, Mr. Chairman. You can't.

McCaul: You can't.

Toohey: You cannot.

McCaul: So as a result of this legal policy or analysis that was done, we probably have God knows how many counterfeit chips coming into this country and we're excluding the private sector from being able to assist DHS in identifying counterfeit chips coming into the country, is that correct?

Toohey: That's exactly correct Mr. Chairman. We're desperate to help. We've been begging Treasury and DHS to let us help stop these dangerous chips that are coming in.

McCaul: Well we can try to help you, I hope Mr. Thompson. I don't see this as a Republican or Democrat issue, I see this as just a common sense issue that I hope perhaps we can work together to change this policy. Otherwise we're going to have counterfeit goods coming in that can't be identified.

McCaul: I want to try to hit a quick question with each of you; I know my time is limited. But going to Mr. Russo, I talked about the example of just one drug going to so many different countries around the world and finally ending up in the United States being counterfeit, and we talk about this chain of supply. What do you consider to be the greatest threat to pharmaceutical companies, to the supply chain?

Russo: Mr. Chairman, the greatest threat that we see to the supply chain is what's available over the internet. The ease in which a consumer, wherever it is in the world, can order counterfeit pharmaceuticals over rouge websites presents a significant threat to patients in the United States, and for that matter, other countries.

McCaul: And you know, there's been some talk about making it legal for people to import from Mexico and Canada, does that pose any threat in terms of the quality of the product?

Russo: The problem is that when you look at internet sites that sell pharmaceutical products, what you look at is a very slickly designed website with a person in a white coat with a stethoscope around their neck, the patient throws a credit card in there and orders product and you really don't know what you're going to get. You could get diverted products you could get stolen products, you could get counterfeit product, and as you said in your remarks sir, those products are less than efficacious and don't treat disease. So that's the issue. You have a slick front and you don't know what's behind that and as we purchase from those sites we find that many of those products to be substandard coming into the United States.

McCaul: Do you know what percentage of these consumers are seniors that buy their medications online?

Russo: No, Mr. Chairman, I don't have that data. We see a lot of different consumers buying over the internet for various reasons.

McCaul: If I could move on to Mr. Mancuso. In my prior life I worked at the Department of Justice, we worked quite a bit on export control like cases, dual-use technologies, so I'm very familiar with that. Most of these cases involved China. And we know that the most probably hacked into office, from a cyber attack, is this export control office within the Department of Commerce, for obvious reasons. What more needs to be done to protect… we don't want to slow commerce down, but we certainly don't want to be giving nations that don't have our best interests at heart technology, like the example I gave, one it's a medical device, but then it can be used for a nuclear device. What more needs to be done?

Mancuso: Mr. Chairman, I would suggest to begin with to distinguish two things. First is refining our export controls and reaching out to industry to ensure that the private sector is really a partner in enforcement. Many U.S. companies want to help and have more information at their disposal with respect to industry competitors who may not be complying with the law. On the other hand, there is industrial espionage, which is of course different because industrial espionage is the intentional theft of technology. I think we have to, specifically with respect to state-based competitors, near pier competitors, looming adversaries perhaps, we need to buttress our counter intelligence capabilities to figure out what technologies they're interested in and what vectors they use to acquire our technologies. So I would submit to you, Mr. Chairman, that there are two things: export controls and outreach in industries to ensure that, on the U.S. side of the equation, industry knows what is controlled, how it's controlled, how it can be exported. But on the sort of foreign side, we need to build a better firewall in terms of our counter-intelligence capability to uncover and prosecute industrial espionage.

McCaul: Thank you, last question to Ms. McNeill on the worksite enforcement issue. According to the Congressional Research Service, since this administration has come into power, administrative arrests have declined 77%, criminal arrests have declined 59%, and convictions declined 66%. I know that there's a shift in policy in terms of going after employers and not the employees, but these numbers to me are very disturbing in the sense that we are not enforcing the law. What is your opinion?

McNeill: Well, it's sometimes very difficult, Mr. Chairman, to disaggregate these employers of illegal labor from the illegal workers. If you look at the situations where they, if they are in the Bush administration during worksite arrests, they may find individuals who, either the employer had knowledge of the identity theft ring that was going on, that the employers were maybe violating other workplace standards, other immigration laws in the workplace. And these illegal workers were so essential to providing that kind of case to be able to prosecute employers. So, you can't take one and not have the other to have an effective enforcement strategy. You really have to do both because they work off of one another. It's an economic problem because workers need jobs; employers need labor, so we have to attack it from both sides.

McCaul: And this hearing is really about protecting intellectual property and innovation in this country and protecting American jobs; jobs that Americans would have but they're losing. And so, E-Verify always did have great promise if fully implemented, and the verification on Social Security numbers, if we could fully implement that. But, in fairness to both the prior administration and this administration, we have yet to be able to fully implement that program.

McNeill: I would give significant credit, Mr. Chairman, to the Obama administration for taking the time to look at ways to improve E-Verify as a system. They have done E-Verify self check, which essentially allows individuals to go look at their own information. That only helps improve the accuracy of E-Verify, so I think that is an area. But we can't make E-Verify the only centerpiece enforcement tool because it doesn't take into account identity theft and off the books employment, which were huge issues in the workplace.

McCaul: Thank you.

# # #