Remarks by Secretary Napolitano at the Global Cyber Security Conference

SHARE

Release Date: August 4, 2009

Washington, D.C.
Global Cyber Security Conference

Secretary Janet Napolitano: I want to thank the Secret Service, S&T [DHS Science and Technology Directorate]—of our office for hosting this meeting on cybersecurity—an area that has commanded special attention from me in my office since I began my tenure as Secretary. Indeed, even before—at the state level as we repeatedly saw our state systems hacked into—it is not a threat of the future. It is an actuality.

Indeed, it was just about a year ago today that criminal charges came from a Secret Service investigation into the theft and sale of 40 million credit card numbers by an international group of cyber criminals. And that case, I believe, was just the tip of the iceberg in terms of the damage that cyber crime, cybersecurity can entail. We have to look at the landscape now; but, more important, we have to—I think—acknowledge amongst ourselves that in terms of cybersecurity we've been living in a cyber 1.0 world and we need to be cyber 3.0 and beyond. Because the minute we start talking about a particular methodology of cyber the cyber bad guys are already moving ahead. This is a very, very rapidly evolving environment in which real crime and real damage can occur.

So let me, if I might, tell you where the administration is, what we've done, and then solicit some questions. But, as you know, the president ordered a 60-day cyber review and that was designed to say, "Hey—look. We have cyber stuff kind of all through different parts of this big behemoth called the federal government. How do we get it coordinated? How do we get it focused? Who is going to do what?"

And the review concluded that the Department of Defense [DOD] would obviously be in charge of the protection of the dot mil side of the federal government. And then the Department of Homeland Security [DHS] would be in charge of the dot-gov, the civilian side of the government; i.e., everything else and, also, the intersection with the non-government private side's dot-org, dot-com.

When I came into the department I think it's fair to say we were not organized sufficiently where cybersecurity is concerned; that it was just as these efforts were kind of spread throughout the federal government—they were kind of spread throughout the Department of Homeland Security. So I recruited Phil Reitinger to come back into the government. He had been at DOJ [Department Of Justice].

He had gone over to Microsoft and I recruited him back to be the Deputy Under Secretary for Cyber at the Department of Homeland Security—and who put all of our cyber efforts under his directorate so that everything having to do with cyber would be there, including the National Cybersecurity Center [NCSC]. So, if the question is who at the Department of Homeland Security—who do you call—it's either going to be Phil or someone who works for him. If it's a crime—the Secret Service as well—who is our lead agency on cyber?

I asked the question the other day. I said, "Why is the Secret Service involved in cyber? How did that happen?" And I think the answer is significant. The reason the Secret Service is in there evolves from their historical jurisdiction, protecting the security of our currency and our banking institutions—and, of course, financial institutions are one of the prime targets of cyber threats. So, from that historical antecedent—which goes back to the 18th century—we now have the Secret Service being the lead agency on cyber crime throughout the federal government and in the Department of Homeland Security.

Under Phil Reitinger are also the U.S. Computer Emergency Readiness Teams known as US-CERT. They work extensively with the private sector to protect government networks from an increasing number of attacks. I already mentioned the National Cyber Security Center and others we have now recruited and are recruiting out of the private sector in the computer world—the cyber world—to come in and provide their expertise and lend their expertise to us.

I have something called the Homeland Security Advisory Council [HSAC]. It meets with me regularly. It meets—more importantly—with our upper staff regularly. We actually put a well-regarded former hacker and asked him to come over from the dark side for a little bit and help us there, so that we are reaching out into different worlds to move from that cyber 1.0 environment into cyber 3.0 and beyond. We are also part of the International Watch and Warning Network [IWWN], which includes 15 countries and of course that is very, very important. And let me just pause a moment there. The cyber involvement knows no national boundaries. It knows no nation or state organization. It, in short, is not organized the way we are organized.

We are organized in nice categories, and even in an international environment we are organized in these kind of international organizations—none of which fits cyber and cybersecurity. And that's exactly what I mean when I say we need to move creatively from the 1.0 to the 3.0 world. In the Secret Service—and there are many Secret Service I know in the audience today—they have done some incredible work in the cyber environment.

The Electronic Crimes Task Force [ECTF]—of which there are 28, including one that just opened in Rome—are illustrative of the

kinds of efforts that we need to not only have, but also enlarge. Another innovative thing that the Secret Service is a part of is the National Computer Forensic Institute [NCFI] which is a pilot between the Secret Service and the state of Alabama to provide free of charge training to state and local partners to build cybersecurity readiness in all sectors.

So we've got the international aspect of this and the state and local aspect of this. And, I can say—as the former governor and as an attorney general who started one of the first cyber crime units in the country—how very, very important that is. I myself in my travels internationally have now signed a number of agreements with countries on cyber. But I think it is important to recognize that there is no international structure where cyber and cyber crime is concerned. That is part of where we need to go.

So as we look at moving forward from our historical antecedents to where we are now—the division of responsibilities in the federal government, the things the Secret Service already has done, what are some of the issues that we need to confront? First of all, we need to confront how we really engage our partners. More than just having a conference, what are our actual plans for working together? How are we going to share intelligence from the government to the private sector and back in real time, so that it's useful? How will we work together on a day-to-day basis? How are we going to grow, recruit and retain experts or cyber cops and experts in cybersecurity? In other words, where are the personnel going to come from who are going to help us in this effort—and that's particularly important, because in the cyber world, there is such an easy flow within the private sector.

How do we grow our own cyber experts who will work within a government framework and how do we make sure we will recruit and retain top talent? Our goal at the Department of Homeland Security, quite frankly—between Phil's efforts and the Secret Service—is to be the repository for cybersecurity and to really recruit the best minds in the country. How do we do that? How do we build that capacity? How do we build capacity to keep ahead of the bad guys?

How do we get creative and think not just of what they've done, but what they're going to do next and next and next? And then how do we share those ideas so that we are not chronically playing catch-up where the cyber field is concerned. How do we stay aware and share information about developing threats in the cyber world? How can we continually be more innovative than our enemies would have us be? For those of you who are in academia—how can we fully involve the research and development efforts that you are undertaking in the cybersecurity efforts that we are making?

For example, right now on the military side of things we have a very impressive military R&D [research and development] capacity, but we have much fewer R&D. We don't have that kind of R&D capacity for things like cybersecurity on the civilian side. That's why we have to engage with private sector partners. That's why academia could be very, very important. And how do we engage the American people and build understanding about the cyber threat? The critical issue here is not just for the big players; the entire private sector, but every business in the United States, large or small; every home that has a computer in it and that is, as you know, an increasing number of our homes.

They are now part and parcel; not just who could be attacked, but how we protect ourselves before an attack occurs. So our challenge in moving from 1.0 to 3.0 is how to take the capacity, the wisdom, the intelligence of everyone in this room and outside and harness it in a way that gives us really an ideal protection network across the United States. Now, one activity ongoing now that I want to share with you that you can't help provide input into is something called the "Quadrennial Homeland Security Review," the QHSR.

But the QHSR is modeled after what they do at the Department of Defense. This will be the first one on the civilian side at the Department of Homeland Security and what it is designed to do is to really provide the strategic—not the tactical—but the strategic goals for the Department of Homeland Security over the next four years. And we are very aggressively seeking input into that, because as the newest federal department this could be very, very useful and immediately put to work in terms of how we guide our efforts.

How do you do that and provide input? Well, there's a website, of course. It's called Homeland Security dialogue dot-org; Homeland Security dialogue dot-org—all one word—homelandsecuritydialogue.org. And the input there is being then placed into that QHSR process and also—to the extent something useful is provided on the cybersecurity area from a strategy standpoint into our 2011 and 2012 budget and budget request—so these are the kinds of challenges we have. How do we employ the people here? In the capacities that you have, how do we knit ourselves together more quickly?

How do we share intel on a real time basis and cross our different silos, as it were, to make sure that the protection of the cyber environment—which is not a static target, but a moving one—but that the protection of that environment is and remains a top priority in which we achieve success; so thank you all for what you have been doing. More importantly, I hope I have challenged you to think ahead now about what we need to do in the cyber future. Thank you very much.

###

This page was last reviewed/modified on August 4, 2009.