Tom Bossert

Presser on Presidential Cybersecurity Executive Order

delivered 11 May 2017, White House, Washington, D.C.

[AUTHENTICITY CERTIFIED: Text version below transcribed directly from audio]

Couple of things positive to report today, and the first is that President Trump, about an hour ago, signed an executive order on cybersecurity. And that executive order, among other things, is going to keep his promise that he has made to the American people to keep America safe, including in cyberspace.

I'd like to do a few things. I'll promise you that we will distribute the executive order, but if I could, I'll preview the executive order for you, walk you through its three primary sections, some of its wave tops, and then take your questions.

Among other things, at least as an observation for me, I think the trend is going in the wrong direction in cyberspace, and it's time to stop that trend and reverse it on behalf of the American people. We've seen increasing attacks from allies, adversaries, primarily nation states but also non-nation state actors, and sitting by and doing nothing is no longer an option. So President Trump's action today is a very heartening one.

There are three sections. They're in priority order, in a sense. The first priority for the President and for our federal government is protecting our federal networks. I think it's important to start by explaining that we operate those federal networks on behalf of the American people, and they often contain the American people's information and data, so not defending them is no longer an option. We've seen past hacks and past efforts that have succeeded, and we need to do everything we can to prevent that from happening in the future.

So a few things on federal networks. We have practiced one thing and preached another. It's time for us now, and the President today has directed his departments and agencies, to implement the NIST framework. It's a risk-reduction framework. It is something that we have asked the private sector to implement, and not forced upon ourselves. From this point forward, departments and agencies shall practice what we preach and implement that same NIST framework for risk management and risk reduction.

The second, I think, of...note -- point in protecting our federal networks is that we spent a lot of time and inordinate money protecting antiquated and outdated systems. We saw that with the OPM hack and other things. From this point forward, the President has issued a preference from today forward in federal procurement on federal IT for shared services -- got to move to the cloud and try to protect ourselves instead of fracturing our security posture.

Third point I'd make is that the executive order directs all its departments and agency heads to continue its key roles, but it also centralizes risk so that we view our federal IT as one enterprise network. If we don't do so, we will not be able to adequately understand what risk exists and how to mitigate it.

A number of thoughts on that. Among other things, that is going to be a very difficult task. So modernizing is imperative for our security, but modernizing is going to require a lot of hard, good governance. And responsible for that today is the President's America -- American innovation -- Technology Council, I'm sorry. The President's American Technology Council is going to run that effort on behalf of the President here out of the White House. And we have great hope that there will be efficiencies there, but also security.

And I would probably note to you that other countries have taken two or three years to learn what we just came up with in two or three months, and that is that we can't promote innovation without first thinking through risk reduction. So doing that together is a message that we've learned, but doing it together is a message we'd like to encourage private sector folks to adopt.

So point two in the executive order is our critical infrastructure cybersecurity effort. The President has directed the President's Cabinet to begin the hard work of protecting our nation's most critical infrastructures -- utilities, financial and healthcare systems, telecommunications networks. He's directed them to identify additional measures to defend and secure our critical infrastructure. And he's continued to promote the message that doing nothing is no longer an option.

So the executive order not only requires his departments and agencies to help those critical infrastructure owners and operators and the most important ones, but to do it in a proactive sense. The message is a -- a tilt towards action.

We've seen bipartisan studies, as an observation from me, over the last eight years, both parties. They've made powerful recommendations. They have not been adopted for various reasons. This executive order adopts the best and brightest of those recommendations, in my view.

I'm going to stop with those three and take questions.

Question: Two questions for you real quickly. First --

Mr. Bossert: Actually, if I could --

Question: Yes, please...Brian.

Mr. Bossert: Brian, go ahead.

Question: First, was the Russian hack in any way responsible or an impetus for this? Number two, I've talked to IT people who say putting stuff on the cloud actually can be problematic as far as security. So what additional security measures would you apply to the cloud to make sure that it's not as risky as some of the IT people tell us it would be?

Mr. Bossert: Yeah. Couple questions there. So let me say three things first. The third section of the executive order -- may be the one I skipped over here a moment ago -- speaks to two halves. It speaks to not only the need to develop the norms and the interoperable, open communication system that is the Internet -- the United States invented the Internet and it's time to maintain our values on it -- but it also speaks to a deterrence policy which has long been overdue.

And so the Russians are not our only adversary on the Internet, and the Russians are not the only people that operate in a negative way on the Internet. The Russians, the Chinese, the Iranians, other nation states are motivated to use cyber capacity and cyber tools to attack our people and our governments and their data. And that's something that we can no longer abide. We need to establish the rules of the road for proper behavior on the Internet, but we also then need to deter those who don't want to abide by those rules.

So the answer to your first question is, no, it wasn't a Russian-motivated issue. It was a United States of America-motivated issue.

Question: And the second question about the -- the cloud, that security on the cloud -- IT people say it's --

Mr. Bossert: If we don't move to shared services -- we have 190 agencies that are all trying to develop their own defenses against advanced protection and collection efforts. I don't think that that's a wise approach.

There's always going to be risk. And so your questions is, are we still at risk? Yes. I'm not here to promote for you that the President has signed an executive order and created a cyber-secure world in a fortress U.S.A. That's not the answer. But if we don't move to secure services and shared services, we're going to be behind the eight ball for a very long time.

Question: Thank you.

Mr. Bossert: You're welcome.

Sir.

[crosstalk]

Question: ...You said "sitting around doing nothing." Is it -- Is it your contention that the Obama Administration, that was its approach to cybersecurity? Sitting around and doing nothing? Question one. And number two, you talked about one enterprise network. Does that mean every system throughout the federal government under this executive order, the ambition is to make them all the same? Or protected in the same way?

Mr. Bossert: No. So I'll answer them in reverse order, if I can.

What we need to do is view the federal government as an enterprise, as opposed to just viewing each department and agency as its own enterprise. So the Department of Homeland Security -- and Secretary Kelly will play a large and leading role in this effort in implementing the President's executive order -- has an enterprise. And their enterprise network covers 340 or so thousand employees and their contractors and so forth. They are responsible, and that Secretary of each department and agency will remain responsible, for securing those networks.

But we need to look at the federal government as an enterprise as well so that we no longer look at OPM and think, well, you can defend your OPM network with the money commensurate for the OPM responsibility. OPM, as you know, had the crown jewels, so to speak, of our information and all of our background and security clearances.

So what we'd like to do is look at that and say, that is a very high risk, high cost for us to -- to bear. Maybe we should look at this as an enterprise and put collectively more information in protecting them than we would otherwise put into OPM looking at their relevant importance to the entire enterprise.

Question: So their budget, in other words.

Mr. Bossert: Not just their budget but based on what they do. So each department and agency has a responsibility to protect its own networks, but they now have a responsibility to identify their risk to the White House, to the President, so that we can look at what they've done and, just as importantly, what risk they know they're accepting but not mitigating. There's a lot of identified risk, but there's also a lot of identified and not remediated risk.

So that mitigation strategy is going to have to come through a centralized place. We've seen other countries, Israel and others, adopt a centralized view of risk management and risk-acceptance decisions. So that's the answer to your question.

The second question, though, maybe, is that --

Question: "Sitting around doing nothing."

Mr. Bossert: Yeah, so --

Question: Is that the Administration -- the previous Administration's approach, from your vantage point?

Mr. Bossert: Yeah, no, I think that -- I think that the -- the observation is that we have not done the basic block-and-tackling, right, of thinking of the Internet as something that the American people benefit from. I think what we've done is focus on the federal IT portion of it. I think that a lot of progress was made in the last Administration but not nearly enough. I think we're going to change that. And I think looking at this from the perspective of a deterrence strategy, to be honest, yes, I think the last Administration should have done that, had an obligation to do it and didn't.

Sir.

Question: [Can you speak] a little bit about deterrence? I was wondering if the Administration has a view on what might constitute an act of war with regard -- you know, what kind of cyberattack might -- might constitute an act of war.

Mr. Bossert: Yeah, there's a whole lot that we'll talk about in terms of what constitutes a cyberattack, what's war and what's not war. The Tallinn Manual and other things are important. But I think the most important answer to your question is that we're not going to draw a red line on cyberwar at this point today. It's not within this -- the direct scope of the executive order. But it also would violate, I think, the President's primary mission to me to not telegraph our punches. If somebody does something to the United States of America that we can't tolerate, we will act.

[crosstalk]

Question: You said that -- You said that the [unintelligible] goal of this is to secure, you know, the Internet. You talked about the Internet as something that Americans -- Americans use and enjoy. Well, the technical standards for, you know, most things on the Internet are put together by many, you know, international standards organizations and engineers, and things like that that often aren't in the United States. Has there been any talk of outreach to these sorts of bodies to try and build in security into the next generation of protocols?

Mr. Bossert: Yeah, absolutely. So the message here is not just protecting the people of America. We have an "America first" perspective, but the idea of having likeminded people with similar viewpoints, like our allies, developing with us the open, operable Internet is something key to figuring out how we will define what is and is not acceptable.

We can't cut off the Internet at our borders and then expect it to operate in a viable way. And if there are good ideas coming out of Germany, then we'll take them. If there are good ideas coming out of Peoria, we'll take them as well.

[crosstalk]

Question: You mentioned -- You mentioned the American Technology Council a short time ago. We really don't have much of an indication that there's going to be, like, significant Silicon Valley or tech leaders who are going to be coming here. We know that there have been reports the President's had a few phone calls with someone like Mark Zuckerberg. Can you enlighten us a bit? Who can we expect to see here coming to the White House next month? Can we expect to see someone like Mark Zuckerberg working closely with the Administration when it comes to that council?

Mr. Bossert: Yeah, so let me go backwards a little bit. Instead of telling you who the President did and didn't talk to -- I'll probably get that wrong anyway -- I'll tell you that there's a lot to be learned from private industry. And among other things, that stuff needs to come into the White House in the appropriate way.

And so we talk on a regular basis to leaders, some that are technical leaders, some that are business leaders. My point of calling out the American Technology Council was to point out that they're going to have a leadership role in modernizing our federal IT. And that has a lot of reasons, right? There's efficiencies and cost-savings that are beyond just security. So this executive order speaks to the security component of it. And I would direct you then to the American Technology Council and their efforts as you look through and think about those other efficiencies.

But, you know, as an example, we've heard numbers that suggest the federal government spends upwards of 40,000 dollars per employee on their IT service costs. And that is so out of line with private industry that Secretary Ross and others would probably have a very easy time buying and making a lot of money off of a company that so poorly invested their dollars. And so I think you'll see that innovation come from that group of leaders and thoughtful people.

And then in terms of what you'll see over the next month, I would say I don't know the answer to that specifically, but I'd like to take the opportunity and the opening before Sarah pulls me to thank two or three people, and one of them high on my list is Mayor Giuliani. I'd like to thank him for the advice he's given to me and to the President, to others, as we formulate this thinking. I'd like to thank Representative McCaul. I'd like to thank a few other members of Congress -- Representative[s] Ratcliffe and Hurd; Representative Nunes, Senator Collins, Senator McCain, in particular; Senator[s] Bird and Whitehouse. There is -- I'm sorry, Burr and Whitehouse. There's a number of people that provided thought leadership and taken action to pass legislation -- all those things that we've liked and that has improved our cybersecurity over the last eight years. So I don't want to be critical of things that have happened over the last eight years, but I do want to look forward to improvement.

[crosstalk]

Question: Could you -- a...former Obama Administration official who dealt with other countries and other entities in other countries -- he said that there were tens of thousands of attempts to hack into government systems daily. Can you quantify? Can you confirm or deny that?

Mr. Bossert: No.

[crosstalk]

Mr. Bossert: And the answer for "no" is that we see that happen and we then start getting into a numbers game. And what I think would be a better argument right now -- not to cut off that question, it's a -- it's a reasonable one, but the better answer here is for us to figure out how we can provide a better collective defense of our federal IT and those networks and data that we operate. If we do it based on an individual attack basis, we're probably looking at it in the wrong way.

Question: So was this person correct when they said from entities -- from entities from around the world....

Mr. Bossert: Yeah, I would say it this way, without numbers -- the trend line is going in the wrong direction. We see additional attacks, additional numbers, additional volume, and occasionally additional successes that trouble us. And that's the best way I can quantify that for you today.

Question: Thank you.

Mr. Bossert: Yeah, you're welcome. Thank you.

[crosstalk]

Question: Can you just say why the cybersecurity order was delayed? This was going to come out one day early in the Administration. And there had been a lot of talk about concern from Silicon Valley and tech leaders with the direction that it was going in. So are those -- do you have some sense of the kind of support that this order has, or not, from the tech world?

Mr. Bossert: I want to answer you and even reject part of your question, if I can, right? And I think that will be clarifying. So first, I'll reject one part of your question. So we did see some concerns, but I don't think that they remain. And I'll look forward to their response after they read the President's executive order today.

One of those concerns, for example, arose when they read the voluntary call on the President's executive order, which I applaud today, that we reduce greatly the number of botnet attacks in the United States -- the distributed denial of service attacks. That's going to require voluntary cooperation among all the different owners and operators of different privately held companies -- from service providers to manufacturers of goods. And those things are going to have to happen voluntarily.

What the President calls for is for the government to provide the basis for that coordination, without defining who's in and who's out -- it's a voluntary operation. But we know that they have the technical capacity, if they have the will, to come together on behalf of the American people and reduce those botnets dramatically. And the President's calling for them to do that. He's asking for the Secretary of Homeland Security and the Secretary of Commerce to facilitate that.

And what we thought we saw was reflections of a concern that there would be a compulsion, and I think that that's something that I can put to rest today -- and that's why -- why I poked on your question a little bit.

But then, if I could, the broader question of delay, I don't really much take that either. I think sometimes we've been criticized for doing things too quickly, and now maybe we're being criticized for doing things to slowly. So maybe --

Question: [unintelligible]

Mr. Bossert: -- maybe I'm -- maybe I'm right in the middle -- maybe I'm right in the middle of the sweet spot, I would argue. But I think the President has hit this timing perfectly, and I'll tell you three reasons why.

One of the block-and-tackle things that he directed us to do before the executive order was to get the money right. He's picked a Cabinet full of people that know that business operations and business functions have to -- have to follow first so that you can then provide policy that he can implement, right? So policy sets direction and vision, but if you don't have the right money and back-office infrastructure and so forth to implement those things, well then you have to either change your vision or change your amount of money.

And so, just off the top of my head, I just thought you might ask that question. The first I already preemptively answered -- and that is that we kind of learn a lesson here that we don't want to innovate with policy on the innovation side, and secure with policy on the security side without doing that in tandem. And you saw the President signed on Friday last the Technology Council and he signed today the cybersecurity order. And that was done intentionally.

And then, lastly, in between now and then, the President's FY18 budget allocated 819 million to DHS's cybersecurity budget alone. It -- It dedicated an increase of 1.5 billion across all departments involved in protecting cyberspace.

So, from my perspective, both his first budget request and his future ones have right-sized and aligned that amount of money, keeping America safe. And that might answer all three components of your question.

And with that, I know Sarah wants to pull me away. So thank you so much for your time. Appreciated it.

[crosstalk]

Question: -- the President address concerns Americans might have about political motivations that these cybersecurity companies like -- for instance, you mentioned Facebook -- they're very political -- or Crowdstrike --