President Trump Is Cracking Down on Voter Fraud

Thursday, President Donald Trump signed two very important executive orders relating to the security and integrity of federal elections and the security of the Internet and the federal government's web-based infrastructure.

During the afternoon press briefing, Principle Deputy Press Secretary Sarah Huckabee Sanders addressed the order related to elections:

> This will be chaired by Vice President Mike Pence. The president is committed to the thorough review of registration and voting issues in federal elections. And that's exactly what this commission is tasked with doing.
>
> The bipartisan commission will be made up of around a dozen members, including current and former Secretaries of State, with Kansas Secretary of State Kris Kobach serving as vice chair. It will also include individuals with knowledge and experience in elections, election management, election fraud detection and voter integrity efforts.
>
> Five additional members that have been announced as of today—Connie Lawson, the secretary of state of Indiana; Bill Gardner, secretary of state of New Hampshire; Matthew Dunlap, the secretary of state of Maine; Ken Blackwell, former secretary of state of Ohio and Christy McCormack, a commissioner on Election Assistance Commission.
>
> The commission will review policies and practices that enhance or undermine the American people's confidence in the integrity of federal elections, and provide the president with a report that identifies system vulnerabilities that lead to improper registrations and voting. We expect the report will be complete by 2018.

> The experts and officials on this commission will follow the facts where they lead. Meetings and hearings will be open to the public for comments and input, and we will share those updates as we have them.

Click here to read the text of the elections order.

Also during the afternoon press briefing White House Homeland Security Adviser Tom Bossert the basis for the president's Internet security order and what all it entails:

> 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 of 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 would make is that the executive order directs all its department 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.

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 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 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 …

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 …

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 . 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 …

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—as an enterprise. And their enterprise network covers 340,000 or so 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 jewel, 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 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 …

[E]ach 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 …

I think that the observation is that we have not done the basic block-and-tackling 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 …

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 …

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 as an example, we've heard numbers that suggest the federal government spends upwards of $40,000 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's 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 and 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—Representatives Ratcliffe and Hurd; Representative Nunes, Senator Collins, Senator McCain, in particular; Senators 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.

Click here to read the text of the cybersecurity and web-based infrastructure order. {eoa}