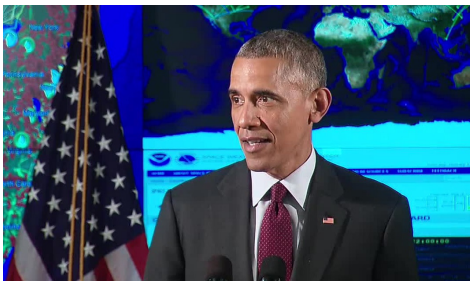
Barack Obama

National Cybersecurity Communications Integration Center Address

Delivered 13 January 2015, Arlington, Virginia



AUTHENTICITY CERTIFIED: Text version below transcribed directly from audio

Good afternoon, everybody. I want to thank Secretary Johnson, Deputy Secretary Mayorkas, and the dedicated public servants of the Department of Homeland Security for welcoming me here today. I've kind of taken over your work space. I apologize for that, but just pretend that I'm not here. I want you to keep working. I did ask who dressed up for this event, and apparently, a few were brave enough to admit it.

But in advance of my State of the Union address next week, I've been rolling out my proposals for keeping our economy on track, keeping it growing, making sure we're creating jobs and opportunity for the American people. And that includes the extraordinary opportunities that exist in our digital economy.

Yesterday, I announced new proposals to better protect Americans from identity theft and to ensure our privacy, including making sure that our kids are safe from digital marketing and intrusions on their privacy based on what they're doing at school. Tomorrow in Iowa, I'll talk about how we can give more families and communities faster, cheaper access to the broadband that allows them to successfully compete in this global economy. And on Thursday, the Vice President will be in Norfolk to highlight the need to continue to invest in the education and skills for our cybersecurity professionals. But today I am here at DHS to highlight how we can work with the private sector to better protect American companies against cyber threats.

Shortly after I took office, I declared that cyber threats pose an enormous challenge for our country. It's one of the most serious economic and national security challenges we face as a nation. Foreign governments, criminals and hackers probe America's computer networks every single day. We saw that again with the attack at Sony, which actually destroyed data and computer hardware that is going to be very costly for that company to clean up. Just yesterday, we saw the hack of a military Twitter account and You Tube channel. No military operations were impacted. So far, it appears that no classified information was released. But the investigation is ongoing, and it's a reminder that cyber threats are an urgent and growing danger.

Moreover, much of our critical infrastructure -- our financial systems, power grids, pipelines, health care systems --run on networks connected to the Internet. So this is a matter of public safety and of public health. And most of this infrastructure is owned and operated by the private sector. So neither government, nor the private sector can defend the nation alone. It's going to have to be a shared mission -- government and industry working hand in hand, as partners.

And that's why I've said that protecting our digital infrastructure is a national security priority and a national economic priority. Over the past six years, we've pursued a comprehensive strategy, boosting our defenses in government, sharing more information with the private sector to help them defend themselves, working with industry through what we call the Cybersecurity Framework not just to respond to threats and recover from attacks but to prevent and disrupt them in the first place.

And that's where these good folks come in. We are currently at the National Cybersecurity Communications Integration Center -- also known as NCCIC. I just got a tour and a briefing. I want to thank everybody here, not just from DHS but from across government and the private sector, because, again, this is a shared responsibility.

This center is one of the critical lines of America's cyber defenses. These men and women work around the clock, 24/7, monitoring threats, issuing warnings, sharing information with the private sector, and keeping Americans safe. So, as a nation, we owe them thanks, and as a nation, we are making progress. We're more prepared to defend against cyber attacks. But every day, our adversaries are getting more sophisticated and more determined, and more plentiful. So every day, we've got to keep upping our game at the same time. We've got to stay ahead of those who are trying to do us harm.

The problem is that government and the private sector are still not always working as closely together as we should. Sometimes it's still too hard for government to share threat information with companies. Sometimes it's still too hard for companies to share information about cyber threats with the government. There are legal issues involved and liability issues. Sometimes, companies are reluctant to reveal their vulnerabilities or admit publicly that they have been hacked.

At the same time, the American people have a legitimate interest in making sure that government is not potentially abusing information that it's received from the private sector.

So all of us -- government and industry -- are going to have to keep doing better. The new legislation and proposals I put forward yesterday will help, especially for a strong, single national standard for notifying Americans when their information has been breached. Today, I want to announce some additional steps.

First, we're proposing new cybersecurity legislation to promote the greater information sharing we need between government and the private sector. This builds and improves upon legislation that we've put forward in the past. It reflects years of extensive discussions with industry. It includes liability protections for companies that share information on cyber threats. It includes essential safeguards to ensure that government protects privacy and civil liberties even as we're doing our job of safeguarding America's critical information networks.

I raised this issue again and the need for this legislation with congressional leaders this morning, including Speaker Boehner and Leader McConnell, and we all agree that this is a threat that has to be addressed, and I am confident that we should be able to craft bipartisan legislation soon to put these systems in place. We're going to keep on working with Congress to get this done. And in the meantime, we're going to do everything we can with our existing authorities to make sure industry gets the information it needs to better defend itself.

Second, we're proposing to update the authorities that law enforcement uses to go after cyber criminals. We want to be able to better prosecute those who are involved in cyber attacks, those who are involved in the sale of cyber weapons like botnets and spyware. We want to ensure that we're able to prosecute insiders who steal corporate secrets or individuals' private information. And we want to expand the authority of courts to shut down botnets and other malware. The bottom line, we want cyber criminals to feel the full force of American justice, because they are doing as much damage, if not more, these days as folks who are involved in more conventional crime.

Finally, and since this is a challenge that we can only meet together, I'm announcing that next month we'll convene a White House summit on cybersecurity and consumer protection. It's a White House summit where we're not going to do it at the White House; we're going to go to Stanford University. And it's going to bring everybody together -- industry, tech companies, law enforcement, consumer and privacy advocates, law professors who are specialists in the field, as well as students -- to make sure that we work through these issues in a public, transparent fashion.

Because they're hard and they're complicated issues. But if we keep on working on them together, and focus on concrete and pragmatic steps that we can take to boost our cybersecurity and our privacy, I'm confident that both our privacy will be more secure and our information, our networks, public health, public safety will be more secure.

We're going to keep on at this as a government, but we're also going to be working with the private sector to detect, prevent, defend, deter against attacks, and to recover quickly from any disruptions or damage. And as long as I'm President, protecting America's digital infrastructure is going to remain a top national security priority.

In closing, I want to say one of the areas I'll be working with Congress is to ensure that we don't let any disagreements keep us from fulfilling our most basic responsibilities. Last week's attack in Paris was a painful reminder that we have no greater duty than the security of the American people. And our national security should never be subject to partisan political games. Congress needs to fully fund our Department of Homeland Security, without delay, so that the dedicated public servants working here can operate with the certainty and confidence they need to keep the American people safe. And that's true across the board in the Department of Homeland Security.

So, again, I want to thank Jeh and Deputy Secretary Mayorkas, and everybody here at NCCIC and DHS for the great job you are doing. You are helping to keep the nation safe and secure.

And with that, we're going to get out of here so you can get back to work. Who knows what's been happening while you've been paying attention to me? All right?

Thank you very much, everybody.