UNITES STATES SENATE COMMITTEE ON
HOMELAND SECURITY
& GOVERNMENTAL AFFAIRS
Senator Tom Carper, *Chairman*

FOR RELEASE: March 7, 2013
CONTACT:
Emily Spain (202) 224-2441 or emily_spain@carper.senate.gov
Jennie Westbrook (202) 224-2627 or jennie_westbrook@hsgac.senate.gov

JOINT HEARING: The Cybersecurity Partnership Between the Private Sector and Our Government: Protecting Our National and Economic Security

WASHINGTON – *Today, Homeland Security and Governmental Affairs Committee Chairman Tom Carper (D-Del.) and Commerce Committee Chairman John D. (Jay) Rockefeller IV (D-W.Va.) convened the joint hearing, "The Cybersecurity Partnership Between the Private Sector and Our Government: Protecting our National and Economic Security." Chairman Carper's opening statement, as prepared for delivery, follows:*

"I am very pleased to be here today with our colleagues from the Senate Commerce Committee hosting a joint hearing on cybersecurity, an incredibly important topic for our country. I would like to thank Chairman Rockefeller, Ranking Member Thune, and my Ranking Member, Dr. Coburn – along with our staff members – for all their work on this hearing. I would also like to thank our witnesses for being here today and for their valuable service to our country.

"I am told that our Committees have not held a joint hearing for over 35 years – since 1975 to be exact. It is fitting that we have come together again to address this issue because we definitely need a true partnership to pass comprehensive cybersecurity legislation in this Congress – a partnership between Democrats and Republicans, the House and the Senate, Congress and the Administration; and, as the title of this hearing indicates, between government and industry.

"We are having this hearing today because America's economy and our national security are under attack. This is not the kind of war that some of us served in earlier in our lives, or read about in history books, or watched on TV. This war is occurring in cyberspace and in real time. Literally as I speak, sophisticated cyber thieves are stealing American ideas and intellectual property – the very innovation that fuels our economy.

"A recent report by Mandiant, an American cybersecurity firm, points the finger for much of this cyber theft to a military unit in China. Even more alarming are the reports that hackers are constantly probing the companies that run our nation's critical infrastructure — our electrical power grid, gas lines, waterworks, and banking system, among others.

"Since this past summer, for example, websites for a number of major U.S. banks have become the target of repeated cyber attacks that have caused disruption and service delays. But once inside a company network, these hackers can do a lot more than steal information or create a

temporary nuisance. Among other things, they can shut down our electric grid or release dangerous chemicals into our water supply.

"We only have to think about the cyber attack that reportedly destroyed more than 30,000 computers at oil giant Saudi Aramco to know this threat is real – and serious. Several of our colleagues, including Senators Rockefeller, Feinstein, and Collins, and the former Chairman of the Committee I now chair, Joe Lieberman, worked diligently to move cyber legislation last year. Unfortunately, the Senate could not come together to pass this vital piece of bipartisan legislation. But given the growing cyber threats that America faces, we are now more determined than ever to put in place a comprehensive cyber policy to protect our nation, its people, its critical infrastructure, and its economy.

"Because of Congress' failure to act last year and the serious nature of the threat, the President issued an Executive Order last month to better protect our nation's cyber networks. Instead of drafting the Order behind closed doors, the White House was very open with the process, conducting numerous "listening sessions," with companies and trade groups so that good ideas could be freely shared and adopted. The final product is an Order that takes a number of critical steps to improve the security of our critical infrastructure.

"One of these steps enhances the way we share cyber threat information between the federal government and the private sector. For instance, in response to the concerns of many in industry, the Order looks to increase the volume, timeliness, and quality of cyber threat information shared with the private sector.

"The Order also relies on a public-private partnership to strengthen the digital backbone of our most sensitive systems. In fact, the Order calls on the private sector to lead the development of new security frameworks in coordination with the National Institute of Standards and Technology.

"Companies may voluntarily adopt the new cybersecurity framework or work with their current regulators on other solutions. To encourage the adoption of any new framework, the Order calls for using carrots instead of sticks. For example, the Order requires the Department of Homeland Security and other federal agencies to establish a set of incentives to promote participation in the program.

"It also requires Homeland Security to expedite the granting of security clearances to the people who run our critical infrastructure, so that industry can better understand the threats they face. Privacy and civil liberties protections are also a key consideration throughout the Order. In fact, agencies are required to incorporate privacy safeguards in all their activities under the Order.

"While I commend the President for issuing this very important Order, there was only so much he could do using the authorities granted to him under existing law. Those authorities are simply not enough to get the job done. Now is the time to begin the process of gathering input from the Administration and a broad array of stakeholders in order to ascertain what Congress needs to do to build on the Executive Order that the President has promulgated.

"For example, we know that more needs to be done on information sharing so that companies can more freely share best practices and threat information with each other, and with the federal government. We should also consider how we can further improve the protection of our nation's critical infrastructure, including offering incentives such as liability protection in certain instances. In addition, we need to modernize the dated process we have in place to ensure the security of our federal networks. This is an area that I have worked on for years.

"It is also important for us to clarify the roles and responsibilities of federal agencies involved in cybersecurity so that we know who should be held accountable for our success or failure in tackling this growing threat. Finally, we must also continue to develop the next generation of cyber professionals and better coordinate our cyber research and development efforts.

"A lot of people in this country of ours question today whether we're still able to set aside our partisan differences when the stakes are high and summon the political will to do what's best for America. I believe this joint hearing is a good step in showing the American people we can. I look forward to working with our colleagues, as well as with the Administration, industry, and other stakeholders, to pass critically needed cyber legislation."

###