ONE HUNDRED TWELFTH CONGRESS

Congress of the United States
House of Representatives

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM
2157 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6143

MAJORITY (202) 225-5074
FACSIMILE (202) 225-3974
MINORITY (202) 225-5051

http://oversight.house.gov

Opening Statement
Ranking Member Elijah E. Cummings

Hearing on "Cybersecurity: Assessing the Nation's Ability to Address the Growing Cyber Threat"

July 7, 2011

In testimony before the House Intelligence Committee earlier this year, then-CIA Director Leon Panetta called cybersecurity "the battleground for the future." Our nation's critical infrastructure—including power distribution, water supply, telecommunications, and emergency services—have become increasingly dependent on computerized information systems to manage their operations and to process, maintain, and report essential information.

Our government's national defense and critical information systems are also becoming increasingly reliant on information technology systems and web-based transactions and services. Successful attacks on these systems threaten our troops, impair vital federal programs, and jeopardize the privacy of citizens whose personal information is maintained in government computer systems.

In the last Congress, Members of the House and Senate introduced at least 50 cybsersecurity-related bills to address these issues. Given the urgency and complexity of these challenges, Congressional leadership called on the Administration to help develop comprehensive cybersecurity legislation. On May 12th, the Obama Administration issued a legislative proposal that would significantly strengthen our ability to guard against cyber attacks. I applaud the President for his leadership on this issue and for creating a strong legislative framework to help Congress complete this important work.

For example, the Administration's proposal would make key changes to the Federal Information Security Management Act, or FISMA, including shifting to continuous monitoring and streamlined reporting for all federal systems. I supported similar legislation last year, and this Committee successfully reported out bipartisan legislation that would have achieved these goals, so I am glad to see the Administration's proposal has incorporated many of the improvements included in that legislation.

There are several provisions in the Administration's proposal that I would like to see strengthened. First, I hope we will consider the creation of a Senate-confirmable official with authority to set administration-wide cybersecurity policy. It is important that the official

responsible for implementing FISMA have the authority to task all civilian departments and agencies with implementation of the federal security standards.

The Administration's proposal also creates a framework to ensure that the federal government and private industry are working together to protect our critical infrastructure. Private industry owns approximately 85% of the nation's critical infrastructure, and the Administration's proposal allows critical infrastructure operators to develop their own frameworks for addressing cyber threats. However, while there is room for healthy debate, even industry agrees that some level of government oversight is necessary to protect the American public from the potentially devastating consequences of a cyber attack. At a recent hearing before the National Security Subcommittee, TechAmerica President Phil Bond testified that education and information-sharing alone are inadequate to protect critical infrastructure and that government "rules, regulations and requirements" are necessary to secure the nation's critical infrastructure.

Other parts of the Administration's proposal attempt to help consumers and companies by creating uniform reporting standards to address cyber attacks that result in breaches of personally identifiable consumer information. However, the proposal also would allow any entity to share with DHS personally identifiable information that otherwise could not be shared under existing law. I agree that we should encourage information-sharing between industry and government, but we also have to be careful that personally identifiable information is appropriately protected and shared with the government only when necessary.

Finally, I agree that law enforcement should have every tool necessary to go after hackers, but I am concerned that the imposition of mandatory minimum sentencing unduly interferes with judges' discretion to set appropriate penalties. I hope that future drafts of the legislation will not include this specific provision.

I would like to thank Chairman Issa for agreeing to include our distinguished colleague, Congressman Jim Langevin, in our hearing today. Jim has been a leader on cybersecurity for many years. As he recently highlighted, the issue of cybersecurity is not a partisan one, but is an issue on which Democrats and Republicans should be able to work together to come up with common sense solutions to help protect the American people.

Mr. Chairman, I look forward to working with you and your staff in a bipartisan manner to update FISMA and pass comprehensive cybersecurity legislation this Congress.

Contact: Ashley Etienne, Communications Director, (202) 225-5051.