For Immediate Release
Thursday, September 10, 2015

Contact: Patrick Boland, (202) 225-4176

Intelligence Committee Ranking Member Schiff Opening Statement in Open Hearing on Worldwide Cyber Threats

Washington, DC – Today, during an open hearing of the House Permanent Select Committee on Intelligence (HPSCI) on Worldwide Cyber Threats, Ranking Member Adam Schiff (D-CA) delivered the following open statement (as prepared):

> "Thanks to each of you for joining us today. I'm pleased we are holding this hearing in open session, and it's telling that both of this Committee's open hearings this year have been on cyber: the challenge of securing our networks – and the related issues of encryption and terrorists' use of social media – are among the most pressing challenges we face.
>
> "The threat to our public and private networks is all too apparent. In the past year alone, we have seen highly publicized hacks of Sony Pictures, just outside my district, intrusions into health insurance providers Premera and Anthem, and the devastating hack into the Office of Personnel Management.
>
> "These three instances, which took place in the context of thousands of other intrusions every day, show the breadth, scale and crippling potential of the threat to our economy, our privacy, and our national security. There are no simple answers to these problems. In fact, some of the steps we can take to better secure our data and our privacy can have unintended consequences. A good example are the largely welcome efforts to make our networks more private and more secure by using pervasive encryption, so that even if hackers steal the data, it would be gibberish without the key to decode it.
>
> "The broader adoption of strong encryption, however, particularly in communications, can simultaneously allow terrorists and criminals to plot in ways that law enforcement and the intelligence community can't access – even with a valid warrant.
>
> "Even open communications on the Internet pose a challenge. Social media has proven a democratizing force throughout the world, but it is now increasingly being used by groups like ISIS to spread messages of hate, repression and violence.
>
> "So, the question is what do we do about cybersecurity, the unintended consequences of encryption, and the use of social media to radicalize?

These are immensely challenging and inextricably linked problems, and I don't profess to know all the answers, nor should anyone in Washington. But, I do want to lay out five principles that should guide our response.

"First, we need to have a broad discussion across industry, government, academia, and the public. Last week I went to Silicon Valley where I had a series of tremendously productive discussions with a number of the leading tech companies. I will continue these conversations, and I encourage others to sit down with them as well. We in D.C. just can't tell tech to 'figure it out.' We have to work with them, and others, to find the best mix of incentives, standards, and technological solutions.

"In these discussions, we in government must also recognize the legitimate economic considerations of our globally-oriented tech sector and the excellent work they are already voluntarily doing to address these issues.

"At the same time, all of us need to recognize the legitimate need of the populace for privacy, the legitimate need of law enforcement and intelligence personnel to keep us safe, and industry's legitimate need to protect intellectual property from hackers.

"This collaboration should also take place on a technical level. I'm pleased to see government agencies like DHS and NSA, for example, continue to partner with universities through grants and cyber challenges to develop safer and more secure technologies and to deepen this country's cyber literacy. We need to do more of this academic and technical collaboration.

"Second, government and the private sector must take joint ownership of the problem of cyber security. It is no longer enough for senior government officials or corporate leaders to simply call in tech support, nor can we afford leaders who take pride in not understanding the technology that underpins their organizations.

"Third, we must grow the government's cadre of cyber experts. We must invest in and attract the best, the brightest and the most creative to work on behalf of the nation's security. The digital revolution was made possible through the marriage of technical savvy and creativity – art and science. Those who could identify the need, and those who could fill it. We must keep this in mind as we develop our bench of cyber experts.

"Fourth, we must develop and communicate in advance proportionate responses to foreign nation cyber attacks and intrusions to generate a deterrent. For example, in the wake of the attack on Sony, North Korea must face tangible, meaningful consequences, and others must know the potential consequences of future attacks or offensive cyber action.

"Fifth, we need to advance legislation that catalyzes solutions. Our cyber information sharing bill, the Protecting Cyber Networks Act, would do precisely that. This measure would essentially crowd-source solutions to cyber threats by allowing private industry and the government to share malware in order to understand it and create solutions to

defend against it. Already, there are public/private cyber information sharing arrangements which are proving invaluable – be it the Defense Industrial Base or the Energy Department's Cybersecurity Risk Information Sharing Program ("CRISP")—or among the private sector, as in Facebook's Threat Exchange. This legislation which has passed the House and is awaiting action in the Senate, would allow these models to go nationwide.

"Ultimately, the threat of a cyber attack presents no easy solutions. Offense is cheap and relatively easy, while defense is expensive and far more complex. Means of communications that secure our privacy can be used by some to threaten our security, and social networks designed to bring us together can be used to try to tear us apart.

"But these complex challenges are not an excuse to throw up our hands. I believe that through close collaboration and discussion, we can take steps to better secure both public and private networks from intrusion in order to save lives and jobs. I look forward to hearing from our witnesses about how we can do that.

"I thank you Mr. Chairman, and I yield back."

###