Statement for the Record 20 May 2013

Statement of John M (Mike) McConnell

Former Director of National Intelligence

Former Director of the National Security Agency

For Testimony before the House Committee on Energy and Commerce for

A hearing entitled “Cyber Threats and Security Solutions”

Mr. Chairman, Members of the Committee,

It is an honor to appear before your Committee today to offer my views on the important topic of Cyber Threats and Security Solutions. You will see in the series of Op-Eds that I have attached to this statement which have been produced over several years, I have long standing concerns for the security interests of the nation, going back to my days as the Director of the National Security Agency. I encourage members of Congress to consider comprehensive legislation that will create the necessary legal framework required to address and mitigate these threats.

I would like to make three basic points:

1. The nation is at strategic risk from “cyber war” and the potential for “cyber terrorism”
2. There also is strategic risk to the nation from “cyber economic espionage” which currently is bleeding the nation of its competitive advantage
3. Without needed cyber security legislation to frame and force full cooperation across the government and the private sector, we will not achieve the required level of cyber security capabilities to protect the nation and its interests.

Cyber threats are well documented and will not be repeated here except to say that nation-states are creating 1000s of zero-day, cyber tools each year to enable two things and which introduce a third concern:

1. Success in any kinetic conflict with another nation and
2. Success in penetrating computer systems for economic espionage, i.e., to steal proprietary intellectual capital. R&D, innovation, business plans, and source code to obtain competitive advantage. (As you are aware, the US, by policy and practice, does NOT engage in economic espionage.)

3. It is just a matter of time before some of these cyber exploitation and attack tools proliferate to extremist groups who want to change the world order. The equivalent of suicide bombers we have witnessed in recent years could be harnessed as “suicide cyber attacks” on the critical infrastructures of the nation.

While the attached op-eds provide my views on above, I will make the following recommendations for the Committee to consider. These recommendations are made on the basis of my experience for over 45 years in threat intelligence and my experience watching the Department of Defense (DoD) become transformed as the result of comprehensive legislation in 1986 commonly referred to as “Goldwater-Nichols” which forced DoD to operate as a joint unified force in the nation’s defense. All efforts to force jointness and interoperability prior to 1986 had been piecemeal or unsuccessful.

WHAT IS REQUIRED AT A MINIMUM:

1. SHARING OF SENSITVE INFORMATION PRODUCED ONLY BY THE GOVERNEMENT WITH THE PRIVATE SECTOR: The US Government, through its intelligence and law enforcement operations, produces valuable information on the cyber threats. This information, most often, is sensitive or classified on the basis of national security rules for protecting sources and methods developed in World War II and used during the Cold War. Those rules served us well in those periods, but the rules now must be modified to force sharing of sensitive data with the private sector in the new era of global cyber threats. The bill produced by House Permanent Select Committee on Intelligence (HPSCI) and passed by the House addresses these concerns.
2. ADOPTION OF HIGHER CYBER SECURITY STANDARDS BY INDUSTRY: The role of government is to cause creation of the needed higher security standards; the debate will be how? I recommend that legislation be written to allow the private sector to create the standards and the role of government only can be to “agree or disagree” the standards are sufficient. The process needs to be iterative until standards are agreed and there must be a way to evolve and update the standards based on new threats or technology advances.
3. INCENTIVISE THE PRIVATE SECTOR TO ADOPT AND USE THE HIGHER CYBER SECURITY STANDARDS: The legislation should contain provisions to provide “Liability Protection” against suits for data breaches to those private sector firms that adopt and use the agreed cyber security standards.
4. PRIVACY CONCERNS: The US Intelligence Community (USIC) is authorized and tasked to collect and analyze information on foreign intelligence. There are concerns, based on historical precedent, that the Executive Branch might use the USIC to collect or intrude on the privacy of US Persons. These concerns can and should be addressed by legislation that makes collection of information about US Persons without appropriate authorization and oversight illegal. We are a nation

of laws and it is up to the Legislative Branch to frame those laws, provide authorization and appropriations to carry out the law and provide the necessary oversight to ensure those laws are not broken. In my 45 years of experience in the USIC, I have observed, firsthand, how the law drives behavior. If laws are broken, the Constitution leads us through a process to address any wrong doing.

Mr Chairman, Members of the Committee, thank you again for the opportunity. I look forward to your questions.