Ranking Member Yvette D. Clarke (D-NY) Opening Statement

Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies
Committee on Homeland Security

"Oversight of Executive Order 13636 and Development of the Cybersecurity Framework"

Thursday, July 18, 2013

Our country's reliance on cyber systems covers the waterfront, everything from power plants to pipelines, and hospitals to highways have increased cyber connections dramatically, and our infrastructure is more physically and digitally interconnected than ever. Yet for all the advantages interconnectivity offers, our nation's critical infrastructure is also increasingly vulnerable to attack from an array of cyber threats.

It is vital that we, as a country, take action to strengthen our national policy on critical infrastructure security and resilience, and includes measures to strengthen cybersecurity. Because the majority of our critical infrastructure is owned and operated by private companies, the public and private sectors have a shared responsibility to reduce the risks to critical infrastructure through a stronger partnership.

The current federal legislative framework for cybersecurity is complex, with more than 50 statutes currently addressing various aspects of it. However, we can all agree that the current framework is not sufficient to address the growing concerns about the security of cyberspace in the United States, and no major cybersecurity legislation has been enacted since 2002, although the executive branch has taken several notable actions.

The federal role in protection of privately held Critical Infrastructure has been one of the most contentious issues in the debate about cybersecurity legislation. There appears to be broad agreement that additional actions are needed to address the cybersecurity risks to CI but there is considerable disagreement about how much, if any, additional federal regulation is required.

So, in February of this year, the President acted through an extraordinary pair of directives, an Executive Order on Cybersecurity and a Presidential Policy Directive on Critical Infrastructure Security and Resilience, that will likely become national and global references for cybersecurity policymaking. Under the EO, the Secretary of Commerce is tasked to direct the Director of NIST to develop a framework for reducing cyber risks to critical infrastructure. The Framework will consist of standards, methodologies, procedures and processes that align policy, business, and technological approaches to address cyber risks.

The Department of Homeland Security, in coordination with sector-specific agencies, will then establish a voluntary program to support the adoption of the Cybersecurity Framework by owners and operators of critical infrastructure and any other interested entities.

It is important that the U.S. set a positive example regarding the essential role that global standards play for both industry and government. This framework presents an important opportunity to develop a product that many other countries can replicate and use in their policy environments. The U.S. could encourage global acceptance of this framework by seeking comments and support from our allies during its development. This adoption would be beneficial by creating consistent and cohesive approaches across those geographies as well as a commitment to the global standardization process.

A long-standing concern of mine is how we go about addressing Cyber Workforce considerations and how they will be they included in the development of the Framework we will be talking about today. Our national cybersecurity workforce must be trained and be able to maintain the skills necessary to understand the changing operating environment. They must also be able to understand the threats and vulnerabilities to that environment, and most importantly, they must be skilled at practices to combat those threats and vulnerabilities. I am hoping that the Chairman and I can work together on this important need.

We also have a need for improvements in the fundamental knowledge of cybersecurity. New solutions and approaches have been recognized for well over a decade and these discoveries were a factor in the passage of the Cybersecurity Research and Development Act in 2002. However, that law focuses on cybersecurity R&D by NSF and NIST. The Homeland Security Act of 2002, in contrast, does not specifically mention cybersecurity R&D, but DHS and several other departmental agencies make significant investments in it. About 60% of reported funding by agencies in cybersecurity and information assurance is defense-related, and we need to direct some of this R&D in the civilian arena. I understand the Chairman has some language along this line, and I hope we can work together on this issue too.

What we all want from a Cybersecurity Framework is something that is flexible, repeatable, performance-based, includes strong privacy and civil liberties protections, and something that is cost-effective. After all, the President is attempting to help the privately held owners and operators of the nation's critical infrastructure to identify, assess, and manage cybersecurity-related risk while protecting business confidentiality and individual privacy and civil liberties.

In short we need to regain sovereignty over our national and local assets that keep our small businesses running, our city and state governments providing services to citizens, our factories humming, and our essential services protected. I look forward to the testimony today to hear about the progress that is being made because of the President's leadership on cybersecurity, and I hope that Congress can learn some lessons from the process he has set into motion.