

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

Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies

Open markup session

Wednesday, September 18, 2013, 10:00 a.m.

Today's subcommittee markup is an important one. We will consider two pieces of legislation that seek to enhance our national cybersecurity and critical infrastructure protection efforts. And, we're doing it in a bipartisan fashion.

As you mentioned, your bill, H.R. 2952, directs the Department of Homeland Security to develop a strategic plan for the overall direction of Federal physical and cyber research and development efforts in furtherance of critical infrastructure protection. The bill also wisely seeks to leverage private sector capabilities through provisions to promote public-private consortiums, and a technology clearinghouse for rapidly changing, proven technology solutions.

Mr. Chairman, later, I will be offering a narrow amendment that I believe will improve the bill. Should my amendment be adopted, I would ask that you add me as a cosponsor of your legislation. I am also pleased that today we are considering legislation I introduced to address fundamental cyber workforce challenges at the Department of Homeland Security, the lead Federal civilian agency for cybersecurity.

My bill, H.R. 3107, The "Homeland Security Cybersecurity Boots-on-the-Ground Act," does a number of things to help DHS identify its workforce needs and address them. Today, many of the Department's top cyber positions are filled by non-permanent contractors and DHS reports having difficulty competing with other executive branch agencies, and the private sector for talent.

In an effort to address DHS' workforce challenges, the Department asked the Homeland Security Advisory Committee to assemble a "Task Force on Cyber Skills" to provide recommendations on the best ways DHS can foster the development of a national security workforce and how DHS can improve its capability to recruit and retain cybersecurity talent.

The "Homeland Security Cybersecurity Boots-on-the-Ground Act" seeks to address a number of the Task Force's key recommendations. Specifically, it requires DHS to develop and issue comprehensive occupation classifications for the Department's cybersecurity missions, and make these classifications available to other Federal agencies. Cybersecurity is a complex mission for the Department and requires a wide range of talent at all levels; given the urgent nature of DHS' recruitment efforts, it is essential that the Department have basic job classifications.

The second key element of my bill is a requirement that the Department assess the readiness and capacity of its workforce to meet its cybersecurity missions. DHS has to identify where positions are located, whether these positions are vacant, held by full-time employees, or contractors. The urgent need to fill critical national security positions often leads to an over reliance on contractors. This workforce crisis can be blamed, at least in part, for creating conditions that allowed Edward Snowden and, now, Aaron Alexis to access Federal information and sites.

Additionally, DHS has to report on the extent to which it has exercised special hiring authority to fill these positions.

The third key element of my bill is the requirement that DHS have a workforce strategy to enhance readiness, capacity, training, recruitment, and retention of the Department's cyber workforce.

Finally, my bill tackles a key vulnerability associated with the reliance on contractors—the protection of classified information. Specifically, it requires DHS to establish a process to verify that cyber and IT contractors receive initial and recurrent security training to protect cybersecurity information maintained by the Department.

Before I close, would just like to acknowledge that there is a lot of interest on our side of the aisle to make progress on these issues. I know that Mr. Keating has a particular interest in nuclear power plant security and Mr. Horsford has shown great initiative with respect to cybersecurity workforce issues. In fact, he has a legislative proposal that I think compliments what I have tried to accomplish with my bill.

More broadly on the issue of cybersecurity, I would reiterate that Democrats stand ready to work in a bipartisan fashion to provide DHS with the authorities it needs and to bolster the cybersecurity of critical infrastructure. In fact, my neighbor from New Jersey, Mr. Payne, has legislation that I would hope this Subcommittee could consider at a later date that tackles a key area of concern—the Smart Grid.

I urge the Members of the Subcommittee to support the bills we are considering today, and I look forward to continue to work with you Mr. Chairman, on issues of importance to our critical infrastructure and cybersecurity.