Opening Statement of Ranking Member Cedric L. Richmond

Cybersecurity and Infrastructure Protection Subcommittee Joint Hearing

Examining DHS' Efforts to Strengthen its Cybersecurity Workforce

March 7, 2018

Since this is our third hearing on cyber workforce, I assume that most of us understand the gravity of failing to fill cybersecurity vacancies throughout the Federal government and, in particular, at DHS. So, let me start by saying the same thing I have said at the last three hearings –

First, if we're serious about 'right-sizing' the Federal government's cyber workforce we need to look beyond four year universities. There is untapped talent in unconventional places, and we will find it if we look for it.

Second, we need strong and consistent leadership from the White House. The President must come out and say that the cybersecurity posture of the Federal government has a direct impact on our economy, our national security priorities, our critical infrastructure, and even the integrity of our elections.

And finally, we have to improve morale at DHS so it can recruit and retain that cybersecurity talent it needs to carry out its mission.

With respect to DHS' cyber workforce, Congress has been responsive. We heard DHS when it told us that it was having trouble competing with the private sector for top cyber candidates, and in 2014 we gave DHS the authority for faster, more flexible hiring.

But we also realized that DHS can't manage what it doesn't measure – so, we directed it to perform a three-step process to assess its own cybersecurity needs:

Step 1 – identify its cybersecurity positions;
Step 2 – bring those positions into alignment with formal OPM data standards, so it can track where cyber positions are located within the Department and start to address skills gaps;
And Step 3 – identify any areas where there are serious gaps in workforce capabilities, or areas of "critical need."

This assessment is supposed to inform a comprehensive cybersecurity workforce strategy that includes a multi-phased recruitment plan - targeting a range of potential candidates from experienced professionals, the unemployed, and disadvantaged communities – to build a more robust cyber workforce at DHS. This workforce strategy would, in turn, inform the broader Department-wide Cybersecurity Strategy required under legislation I authored in 2015.

But DHS has yet to complete its cybersecurity needs assessment and the deadlines for both these strategies has long passed -- yet neither strategy has been delivered to Congress. In fact, this is the third Congressional hearing where I have asked about the status of the Department-wide Cybersecurity Strategy that was due in March 2017.

I expect that today, I will hear the same excuses I have heard every other time I have asked about the DHS Cybersecurity Strategy: DHS plans to release the strategy soon, but the new leadership – and there is, once again, new leadership – needs a chance to review it. As much as I understand the need to let the new administration set its own policy, we cannot ignore the fact that these delays are undermining DHS' ability to carry out its mission.

Moreover, I am troubled by the length of time we are being asked to wait for the reports we need to do our job as authorizers. Despite these ongoing challenges, I look forward to a productive discussion about how we can work together to make sure DHS has the tools, resources, and authorities to maintain a qualified cybersecurity workforce – and do so in a manner that is timely and responsive to Congress.