Statement of Ranking Member Bennie G. Thompson (D-MS)

Joint Hearing:

Interagency Cyber Cooperation: Roles, Responsibilities and Authorities of the Department of Defense & the Department of Homeland Security

Wednesday, November 14, 2018

I would like to acknowledge that yesterday the House passed by unanimous consent H.R. 3359, the *Cybersecurity and Infrastructure Security Agency Act*, and sent it to the President's desk. The bill renames DHS' cybersecurity arm – currently known as the National Programs and Programs Directorate (NPPD) – the Cybersecurity and Infrastructure Security Agency and makes it an operational component – akin to FEMA or TSA.

This legislation has been a long time coming and sends a clear message to agencies across the Federal government and the private sector alike: DHS is the lead civilian cybersecurity agency. Although Congress designated DHS as the primary hub for cyber information sharing in 2015, ongoing attempts to siphon away DHS' Congressionally-mandated role in this space have stalled its efforts to mature into the agile civilian cybersecurity agency Congress envisioned and the threat demands.

I am hopeful that the enactment of H.R. 3359 will help clarify DHS' cybersecurity mission and quash efforts to chip away at it so we can finally shift our focus from "who is doing what" to "how can we do it better."

We are here today to explore the important collaboration that exists between the Department of Defense and DHS to improve the security of the cyber ecosystem. This hearing comes at a time when the Administration is seeking to expand DOD's role in protecting critical infrastructure from cyber threats – which has been a DHS responsibility - and directing DOD to undertake a more offensive cyber posture.

These themes, articulated in the long-awaited National Cybersecurity Strategy and the 2018 DOD Cyber Strategy and Cyber Posture Review, raise important questions about how DOD and DHS will coordinate on issues related to engaging with the private sector and assessing the potential consequences of offensive cyber activity.

As cyber threats continue to evolve and cyber actors grow more sophisticated, the Federal government will need to leverage both the cyber personnel, capability, and budget DOD brings to the table as well as the civilian cybersecurity authorities Congress has conferred upon DHS. However, we cannot allow this collaboration to blur the lines of the roles and responsibilities Congress has established.

Toward that end, I will be interested to learn more about DOD's engagement with the financial services sector through the "pathfinder" program. In particular, I would like to understand how DOD worked with DHS to establish the program and how agencies are continuing to coordinate with the financial services sector.

Finally, I think it important to acknowledge that the entities sitting before us today operate with vastly different budgets and resources. In the past, DHS critics were skeptical that DHS was equal to the task of its mission, and have argued the cyber responsibilities should be moved to agencies perceived to be more competent. I wholly disagree with that notion. That said, it is important to note that despite increases in appropriations for cyber activities at DHS, it has not enjoyed the same level of funding as other agencies.