Statement of Chairman Michael McCaul (R-TX)
Homeland Security Committee

"The Current State of DHS' Efforts to Secure Federal Networks"
March 28, 2017

Remarks as Prepared

I look forward to hearing from our witnesses today on this essential aspect of the DHS cybersecurity mission, protecting our federal civilian networks.

Just last week, our Committee heard from top former cyber and national security officials, including General Keith Alexander, that we must rise to the challenge in combating growing cyber risks and that we must up our game on defense.

We heard about the wide range of cyber threats we face from nation-states, hacktivists and criminals.

Russia meddled in the 2016 Presidential election and Russian intelligence agents were indicted in the massive breach of Yahoo.

North Korea attacked Sony pictures.

Iran hit the financial sector.

China continues to be one of the nation's top cybersecurity threats and, as we all remember, in 2015, Chinese hackers stole 20 million security clearances—including my own—in a breach of the Office of Personnel Management.

And, recently, the alleged hack of the CIA has Wikileaks publishing over 8,000 pages of documents with some of the most highly sensitive cyber weapons.

These blinking red alarms are the reason we are here today. We need to ensure that our federal departments and agencies are properly defended from attacks; we do NOT have time to wait.

Over the last several years, I have championed a number of bills that put DHS in the lead for operationally securing the "dot gov" domain, helping to better protect critical infrastructure, hiring cyber talent at NPPD, being the hub for cyber threat information sharing, and providing voluntary assistance to the private sector.

In late 2015, the Cybersecurity Act became law and included language authorizing DHS to deploy intrusion detection and prevention capabilities and to support its continuous diagnostics and mitigation endeavors across the federal civilian enterprise.

The law requires federal agencies to utilize the intrusion detection and prevention capabilities and at the end of last year, the Department announced it was providing cybersecurity services to 93 percent of the executive branch's civilian workforce.

But perimeter detection is only one part of what needs to be a larger and more holistic defense-in-depth strategy and architecture.

DHS must adopt an entire suite of tools and technologies while ensuring its capabilities are keeping up with the evolving cyber threats that we discussed at last week's cyber threat hearing.

As I mentioned last week, this Committee will be moving legislation soon to create a stronger, consolidated cybersecurity agency at the Department of Homeland Security. This proposal will elevate the cybersecurity mission at DHS and further enhance cyber operations, including those to more effectively secure federal networks.

This will help us step-up our cyber defense efforts and attract top talent.

And we have already begun to work with DHS and others to make that a reality.

Today, I hope to hear from DHS about how it is working to protect our federal departments and agencies from these sophisticated cyber threats and what more assistance may be needed. As I'm sure everyone here can agree, we cannot afford another OPM-style breach, we must better ensure our nation's most sensitive information is protected without any delay.

###