Committee on
HOMELAND SECURITY
Chairman Michael McCaul

Opening Statement

June 24, 2015

Media Contact: Susan Phalen
(202) 226-8477

Statement of Subcommittee Chairman John Ratcliffe (R-TX)
Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies

"DHS' Effort to Secure .Gov"

Remarks as Prepared

The Subcommittee meets today to hear what the Department of Homeland Security is doing to secure the U.S. government's networks from cyber hackers. The magnitude of the latest breach at the Office of Personnel Management (OPM), and the impact it will have on tens of millions of Americans and our national security for decades to come, is simply unacceptable. OPM was warned about its poor IT security; yet we still found them asleep at the switch. To put it into perspective, OPM was responsible for safeguarding extremely sensitive data—personnel files and security clearance information for tens of millions of federal employees—yet OPM's efforts to secure its network were laughable. The stakes were immense, yet the cybersecurity efforts were pathetic. In my opinion, this could be classified as a "cybersecurity malpractice" of sorts. The federal agency guarding this sensitive information demonstrated gross negligence and willful disregard of earlier warnings. We need to know who in this Administration is in charge, and who is responsible for securing our federal government's civilian information systems.

The nature of the compromised data is particularly concerning because it contained the personally identifiable information (PII) of up to14 million Federal and Congressional employees, and military personnel. Not only did we fail to protect PII, we failed to protect the security clearance background check information contained on the Questionnaire for National Security Positions form, called an SF-86. The individuals who serve our country, often risking their lives, disclose substantial personal information on these forms to get special clearances to handle our government's secrets and expect their information will be safe.

As we've learned, OPM struggled to implement even the most basic network security protocols. This was spelled out in a November 2014 Inspector General report, one month before the breach occurred. The Government Accountability Office has drawn similar conclusions. Specifically, the IG found lackluster information security governance and even recommended that OPM shut down all its

information systems that lacked a valid authorization. Additionally in 2014, DHS presented to OPM a mitigation plan with recommendations for improving its information security. The question, then, is why the recommendations from DHS and others were not required and fully implemented by OPM?

Unfortunately, the White House response to the OPM breach has been extremely disappointing. The federal government was attacked, yet there is no indication that there will be consequence for these actions. Additionally, the U.S Chief Information Officer Tony Scott has called for a "30 day cybersecurity sprint" for federal agencies to secure their networks and data. The White House is essentially calling on federal agencies to do in the next 30 days what they were already required to do. Our country's cybersecurity should not be a sprint exercise; but rather a marathon—a long, sustained, and comprehensive effort to protect our country from escalating and rapidly evolving cyber-attacks. This Administration's response is not serious and does not reflect the gravity of the threats facing our nation in cyberspace.

It is clear that the nation is under siege by state and non-state actors, and our defenses at OPM and in the federal government are woefully inadequate. As such, today we will examine the cyber capabilities that DHS is providing to OPM and other federal civilian agencies, how quickly these tools are being deployed government-wide, and ultimately, what vulnerabilities and gaps remain in our cybersecurity posture.

Last December, Congress passed the Federal Information Modernization Act (FISMA) to give DHS the authority to carry out the operational activities to protect federal civilian information systems from cyber intrusions. Now that DHS has these authorities, we want to hear how DHS plans to execute the new law and rapidly implement its binding directives and other federal information security capabilities to more quickly secure the .gov domain. Additionally, DHS' Einstein and Continuous Diagnostics and Mitigation (CDM) programs were designed to protect federal civilian agencies' systems, yet not every federal agency has adopted them. Why is that the case? Although these programs are not a silver bullet to preventing further cyber attacks, both play a vital role in what should be a "defense in depth" cybersecurity strategy. Now more than ever, DHS needs to rapidly deploy its cyber capabilities, and show strong leadership to protect our government's networks and most sensitive information from cyber hackers.

I also hope that if nothing else, this latest attack will prove to be a catalyst to get the Senate to act and pass the strong and bipartisan House-passed cybersecurity information sharing legislation. These bills would, in part, authorize DHS' Einstein program and allow for greater sharing of cyber threat indicators so both the public and private sectors can more effectively block known and malicious cyber intrusions.

From my vantage point as Chairman of this Subcommittee and a former terrorism prosecutor, cybersecurity is national security. The U.S. government is under cyber-attack from nation states and criminal groups and I look forward to hearing from our witnesses today on what the Department of Homeland Security is doing about it.

###