October 16, 2018

The Honorable Richard Burr
Chairman
Senate Intelligence Committee
Washington, DC 20510

The Honorable James Inhofe
Chairman
Senate Armed Services Committee
Washington, DC 20510

Dear Chairman Burr and Chairman Inhofe:

We are writing to urge you to formally investigate reports that Amazon cloud computing systems were exposed and left vulnerable to Chinese hackers. These allegations raise serious concerns about whether Amazon and its subsidiary Amazon Web Services (AWS) should be eligible to continue hosting some of the most sensitive information and workloads for the United States government, particularly as the company bids to be the sole Department of Defense cloud services provider for the next decade. Further, we ask that you examine the national security implications of AWS's increasing cooperation with the Chinese government, while simultaneously providing services to the United States Intelligence Community (USIC).

FFMI is a non-profit coalition focused on supporting a modern, fair marketplace that serves the best interests of small businesses, local communities and everyday Americans. Our coalition holds the safeguarding of personal data as a core value in order to ensure that our communities remain safe from breaches and malicious activity. We are deeply troubled by the claims that Amazon cloud computing systems may have been compromised, and are calling for a hearing to get answers on behalf of millions of Americans who may have been put at risk if these systems were exposed.

Elemental Technologies, which was acquired by Amazon in 2015 for $350 million, was reportedly compromised by Chinese hackers who were able to plant a microchip into the company's servers. Elemental's hardware products are used by the Department of Defense, Central Intelligence Agency and the Navy, and a breach of this magnitude would give one of our most closely-watched adversaries access to classified government information.

While the company denies these serious accusations, there is no question that as Amazon's cloud computing services for government agencies have ramped up in recent years, so too have high-profile exposures of sensitive data the company has been tasked with protecting. AWS previously left huge amounts of Pentagon data unprotected in 2017 when its servers were left accessible. Additionally, more than 60,000 files were leaked from AWS servers containing government information that was "highly likely" to be downloaded by malicious actors.

Meanwhile, in mid-November 2017, AWS announced the sale and transfer of their China-based cloud computing infrastructure to Beijing Sinnet Technology Company, a corporation which is primarily headed by high-level People's Liberation Army scientific researchers. The technology and hardware sold by AWS to Sinnet is identical to that deployed to the USIC, effectively providing the Chinese security complex with testing ground for exploiting American national security systems.

AWS furthered their cooperation with the Chinese government just last month through the establishment of the AWS AI research institute in Shanghai. The first such institute in the Asia-Pacific, it will conduct multi-language natural language processing research centered on Mandarin and provide an open source deep learning ecosystem to help machine learning applications.

Amazon is also currently bidding to be the sole provider of cloud services for the Joint Enterprise Defense Infrastructure (JEDI) program, a contract that could be worth as much as $10 billion over the next decade. However, numerous cybersecurity experts have called into question the security of having a single provider protecting these troves of sensitive national defense secrets. In the wake of an alleged hack of this scale, the immense vulnerabilities with this winner-take-all contract design — particularly being awarded to a company with an alarming history of breaches — are abundantly clear.

Although Amazon has previously testified on a variety of issues, its cybersecurity practices have never been formally scrutinized in the context of these contracts. Given the national security implications of these breaches and potential future ones, Congress cannot simply take Amazon's word when it comes to its cybersecurity protocols. It would be unthinkable for an American defense contractor, employed by the Department of Defense, to provide a fully operational weapons system to the Chinese government — we must not allow AWS to continue to provide the Chinese government with technology that they simultaneously provide to our own government. Putting the company under oath will ensure that the American people get the truth about what the company is or is not doing when it comes to putting meaningful cybersecurity protocols in place.

While we are encouraged by the growing number of lawmakers who have raised concerns about these issues, we urge Congress to conduct a formal investigation to ensure that Amazon is held accountable for these privacy lapses. There is too much at stake for our communities for Congress to remain on the sidelines.

Sincerely yours,

Robert B. Engel
Free & Fair Markets Initiative

cc: Members of the Senate Intelligence Committee
cc: Members of the Senate Armed Services Committee