JASON CHAFFETZ, UTAH
CHAIRMAN

ONE HUNDRED FOURTEENTH CONGRESS

ELIJAH E. CUMMINGS, MARYLAND
RANKING MINORITY MEMBER

Congress of the United States

House of Representatives

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515–6143

MAJORITY (202) 225–5074
MINORITY (202) 225–5051

http://oversight.house.gov

REP. STEPHEN F. LYNCH
Ranking Member
Subcommittee on National Security
"Digital Acts of War: Evolving the Cybersecurity Conversation"
July 13, 2016 at 1:00pm in 2154 RHOB

Thank you, Mr. Chairman. I'd like to thank you, Chairman DeSantis, and Ranking Member Kelly for holding this hearing to examine critical strategic and policy issues relating to cybersecurity. I'd also like to thank our witnesses for helping this Committee with its work. Given the sensitive nature of today's topic, I understand that certain questions that may be raised during our discussion would best be answered in specific detail in a secure setting. To this end, I appreciate the willingness of our Administration witnesses to conduct a classified briefing for Committee Members at a date to be determined.

As underscored by National Intelligence Director James Clapper in his most recent Worldwide Threat Assessment of the U.S. Intelligence Community, continuous innovation in cyber and information technology has been accompanied by the emergence of new and complex national security threats. According to Director Clapper, "*devices, designed and fielded with minimal security requirements and testing, and an ever-increasing complexity of networks, could lead to widespread vulnerabilities in civilian infrastructures and U.S. government systems.*"

These lapses in cybersecurity are highly susceptible to exploitation by a range of threat sources, including foreign governments such as Russia, China, North Korea, and Iran, who are motivated by cyber-espionage. There is also the threat of cyberterrorism perpetrated by terrorist groups designed to promote online recruitment, propaganda, and

financing activities and incite "lone-wolf" attacks. The S.I.T.E. Intelligence Group reports that the Islamic State actually maintains its own so-called "Hacking Division" or "United Cyber Caliphate," a group of prominent hackers that has already published several kill lists of U.S. military personnel online. Moreover, hackers have repeatedly targeted the U.S. commercial sector for illegal monetary gain and money-laundering.

The continuing onslaught of massive data breaches in the public and private sectors here in the United States and worldwide evidences the complexity, diversity, and far-reaching implications of cyberattacks. Our national cybersecurity framework must be equipped to prevent and mitigate against public sector attacks such as the critical breaches of information technology systems at the Office of Personnel Management in 2015. These cyberattacks did not only compromise the personal identifiable information of over 22 million individuals; rather, as noted by FBI Director James Comey, they also yielded a "*treasure trove of information about everybody who has worked for, tried to work for, or works for the U.S. government.*" The past two years have also witnessed breaches of computer systems at the State Department, the White House, the Internal Revenue Service, and the U.S. Postal Service as well as the reported leaking of sensitive information pertaining to employees at the Department of Homeland Security and the FBI.

At the same time, our cybersecurity defenses must be able to deter and respond to threats targeting private sector companies and motivated by illicit financial gain. It is my understanding that the Federal Reserve is currently leading other U.S. regulators in developing baseline cybersecurity safeguards for U.S. banks in the wake of a February 2016 attack in which cybercriminals successfully transferred $81 million dollars out of the Bangladesh Central Bank to a casino in the Philippines. We have also witnessed the infiltration of computer networks at JPMorgan Chase that compromised the account information of 83 million households and businesses, a $62 million dollar breach at Home Depot that compromised an estimated 56 million payment cards, and multiple cyberattacks against the target retail chain that resulted in the theft of approximately 40 million credit and debit card numbers and the personal information of up to 70 million customers.

Clearly, the national security threat posed by cyberattacks is multifaceted and demands the continued development of cybersecurity policies and operations that are adaptable, modernized, and comprehensive. I look forward to discussing with our witnesses at today's hearing what steps we are taking in this regard.

Thank you, Mr. Chairman – I yield the balance of my time.

Contact: Jennifer Werner, Communications Director, (202) 226-5181.