TED W. LIEU
33RD DISTRICT, CALIFORNIA

COMMITTEE ON THE JUDICIARY

COMMITTEE ON FOREIGN AFFAIRS

Congress of the United States
House of Representatives
Washington, DC 20515–0533

236 CANNON HOUSE OFFICE BUILDING
WASHINGTON, DC 20515
(202) 225-3976

5055 WILSHIRE BOULEVARD, SUITE 310
LOS ANGELES, CA 90036
(310) 652-3095

1600 ROSECRANS AVENUE, 4TH FLOOR
MANHATTAN BEACH, CA 90266
(310) 321-7664

June 28, 2017

Admiral Michael S. Rogers
Director
National Security Agency
9800 Savage Rd.
Ft. George G. Meade, MD 20755-6000

Dear Admiral Rogers,

Thank you for your service. I write in regard to the new global wave of ransomware attacks stemming from the strain of malware known as "Petya," which takes advantage of vulnerabilities in Microsoft Windows software. Security researchers have confirmed that Petya uses the suspected NSA exploit EternalBlue to infect systems, the same conduit through which the May WannaCry ransomware attacks were promulgated. Based on various reports, it appears these two global ransomware attacks likely occurred because the NSA's hacking tools were released to the public by an organization called the ShadowBrokers.

NSA-created malware has now apparently caused many businesses to grind to a halt, targeted critical infrastructure management systems and ATMs across Europe and Asia, and disrupted the global flow of travel and commerce – including at the Port of Los Angeles, where some of my constituents are employed. As of the writing of this letter, no kill switch has yet been identified to stop the spread of this new ransomware attack.

My first and urgent request is that if the NSA knows how to stop this global malware attack, or has information that can help stop the attack, NSA should immediately disclose it. If the NSA has a kill switch for this new malware attack, the NSA should deploy it now.

As a computer science major, my long term fear – which is shared by security researchers – is that this is the tip of the iceberg and many more malware attacks will soon be released based on NSA's hacking tools. Whatever the cause of the ShadowBrokers leak, the fact remains that these classified exploitation tools are now publicly available. I strongly believe it is now NSA's duty to work with appropriate stakeholders to ensure that American citizens, businesses, and government entities are adequately protected from NSA-inspired malware attacks.

Given the ongoing threat, I urge NSA to continue actively working with companies like Microsoft to notify them of software vulnerabilities of which the Agency is aware. I also urge the NSA to disclose to Microsoft and other entities what it knows that can help prevent *future* attacks based on malware created by the NSA.

Thank you for your attention to this urgent matter.

Sincerely,

Ted W. Lieu
Member of Congress