NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND 20755-6000

21 July 2017

The Honorable Ted Lieu
Member, House Judiciary Committee
Sub Committee on Crime and Terrorism
United States House of Representatives
U.S. Capitol, HVC-304
Washington, DC 20515

Dear Congressman Lieu:

Thank you for your letter dated 28 June 2017 regarding the WannaCry and Petya malware activity. I appreciate your strong interest in cybersecurity, and I want to assure you that the National Security Agency (NSA) shares your concern about the threat to the United States and our allies posed by such malware.

Before I respond to your requests, I want to address one important point from your letter. NSA develops cyber tools only to support its legitimate and legal foreign intelligence mission. The responsibility for the WannaCry and Petya malware rests solely on the malicious cyber actors who created and deployed them to extort money and damage victims' systems.

The first request in your letter asks whether NSA is aware of and could deploy a "kill switch" to stop the malware attack. In the early hours of the WannaCry malware attack, it was widely reported that a "kill switch" had been discovered, and straightforward instructions were published and adopted by many users globally to disable WannaCry. The malicious cyber actors responsible for WannaCry, however, quickly deployed a new variant that was "immune" to the "kill switch" and the malware continued to spread. NSA has analyzed WannaCry and assessed there are no other "kill switches" that would disable it. NSA has not identified any "kill switch" for the Petya malware.

As you know, the best defense against such malware activity is for users to ensure that system patches are up-to-date and to use good cybersecurity practices at all times. Malware and ransomware exploit existing vulnerabilities in network and system software. These vulnerabilities are inherent in the programs created by information technology (IT) vendors.

In the case of WannaCry and Petya, malicious cyber actors merged preexisting ransomware and other destructive code with a variety of exploits for publicly-known vulnerabilities. For example, both WannaCry and Petya exploit a vulnerability in Microsoft's Windows Server Message Block Protocol in order to propagate. In March 2017, 2 months before the publicized WannaCry malware activity and 3 months before the publicized Petya malware activity, patches to fix these vulnerabilities were released by Microsoft to the public. Updating operating systems with these patches prevents the spread of the WannaCry and Petya malware through exploitation of this vulnerability.

Soon after these patches were issued, NSA issued cybersecurity advisories that referenced the patches and reminded users to discontinue use of the affected communications protocol. Additionally, NSA partnered with the Department of Homeland Security and other departments and agencies to ensure that the advisories were disseminated widely across the U.S. Government, to U.S. critical infrastructure and key resources, to our partners and allies, and to the U.S. private sector.

Although patches were available and advisories had been issued, WannaCry and Petya were able to take advantage of less secure, unpatched systems globally in order to propagate. Fortunately, there were significantly fewer infected systems in the United States, where legitimate, registered software is updated automatically and good cybersecurity practices are common.

As to your second request, let me also assure you that we do indeed have a longstanding program to work with IT vendors to help minimize these threats, including by disclosing vulnerabilities when appropriate to do so. In fact, NSA has released, after equity review, more than 90 percent of the vulnerabilities that it has discovered in products made or used in the United States. As part of its information assurance mission, NSA also assists in successfully defending National Security Systems and Department of Defense information systems against tens of thousands of cyber threats each day.

NSA will remain vigilant in protecting against potential threats to these networks and will continue to share information relevant to the cybersecurity of the Nation. Thank you again for your correspondence and for your attention to this important issue and our nation's security.

MICHAEL S. ROGERS
Admiral, U.S. Navy
Director, NSA