Bipartisan Bill Introduced in Senate that Seeks to Prevent Attacks on American Cyber-Networks

Democratic Senator Brain Schatz of Hawaii and Republican Senator Ron Johnson of Wisconsin have introduced the "Protecting Our Ability to Counter Hacking Act of 2017," also known as the "PATCH Act of 2017" in the U.S. Senate Homeland Security and Governmental Affairs Committee, following the recent "WannaCry" ransomware attack, with the intention of requiring government agencies to submit any security holes in software products they discover for independent review in order to determine any vulnerabilities that need to be secured, as reported by **HealthCare IT News** and **Reuters**. According to HealthCare IT News, the PATCH Act of 2017 is supported by Republican Senator Senator Corey Gardner of Colorado, Democratic Representative Ted. Lieu of California, and Republican Blake Farenthold of Texas, as well as McAfee, Mozilla, The Information Technology and Innovation Foundation, and New America's Open Technology Institute.

The text of the PATCH Act of 2017 is available for viewing **here**.

The bill would require the establishment of a Vulnerability Equities Review Board comprised of permanent members, ad hoc members, and National Security Council members who are neither of the above, if approved by the President and requested by the Board. The permanent members would include the following:

- Secretary of Homeland Security or the designee of the Secretary, who shall be chair of the Board;
- Director of the Federal Bureau of Investigation or the

designee of the Director;
- Director of National Intelligence or the designee of the Director;
- Director of the Central Intelligence Agency or the designee of the Director; and
- Secretary of Commerce or the designee of the Secretary.

The Ad Hoc Members would include:

- Secretary of State, or the designee of the Secretary, if the Board considers the matter under the jurisdiction of the Secretary;
- Secretary of the Treasury, or the designee of the Secretary, if the Board considers the matter under the jurisdiction of the Secretary;
- Secretary of Energy, or the designee of the Secretary, if the Board considers the matter under the jurisdiction of the Secretary; and
- Federal Trade Commission ("FTC"), or the designee of the Commission, if the Board considers the matter as relating the the FTC.

The purpose of the Board would be to establish policies relating to "whether, when, how, to whom, and to what degree information about a vulnerability that is not publicly known should be shared or released" by government to a non-government entity and the process by which such information should be shared or released to a non-governmental entity. In other words, as **Reuters** reported, the bill is intended an attempt to put the process "into civilian control" and remove such decisions from the purview of the National Security Agency ("NSA").

According to reporting by **ThreatPost**, this bill codifies the process that the White House has long claimed to have in place to evaluate information on security vulnerabilities, but in fact rarely actually has utilized. According to **Threat Post**, in the particular case of the WannaCry attack, the NSA did in

fact tip off Microsoft of the security issue, which allowed Microsoft to make the patch available to customers in advance of the attack.

While the WannaCry attack was initially reported only to have hit Windows machines, according to reports by **ThreatPost**, it is now known that medical devices and industrial control systems have also been hit by the attack, including equipment used in medical radiology facilities.

Reuters is reporting today that, for victims who have not paid the ransom and/or recovered their files, French Researchers have developed a last resort workaround, which will successfully unlock the encryption key for files hit by the attack in certain conditions. According to **Reuters**, Europol has stated on Twitter that its European Cybercrime Centre has tested this tool and confirmed it will successfully recover data in some circumstances. The technical details of this tool can be accessed through the **Reuters** article.