Protecting our Ability To Counter Hacking "PATCH" Act of 2017

"*Building up a huge stockpile of undisclosed vulnerabilities while leaving the Internet vulnerable and the American people unprotected would not be in our national security interest" –Michael Daniel, White House Cybersecurity Coordinator (April 2014)*

Background: The purpose of this bill is to add transparency and accountability to the U.S. government process for retaining or disclosing vulnerabilities in technology products, services, applications and systems.

- The U.S. government is one of the many stakeholders researching and finding "zero day vulnerabilities," which are flaws in technology that are unknown to the vendor.
- Before they're patched, these vulnerabilities are susceptible to hacking and make the technologies that we rely on every day less secure.
- Usually the U.S. government discloses these vulnerabilities to the vendor so that they can be fixed but sometimes it retains them and exploits them for national security purposes.

Bill Summary: The PATCH Act codifies current government practices and includes additional measures to ensure an appropriate balance between protecting the public and our national security requirements, when it comes to vulnerability disclosure. To do so the, the bill:

- Codifies the current Vulnerability Equities Process (VEP).
- Designates the Department of Homeland Security as the Chair of the Board.
- Tasks the Board with developing a policy for how the government evaluates vulnerabilities for disclosure and retention and to, as much as possible, make public this criteria.
- Streamlines the dissemination process by allowing DHS and NIST to utilize its typical process for disclosing vulnerabilities.
- Ensures that in the event a classified vulnerability becomes known, a process is triggered to alert the vendor to facilitate a patch.
- Adds additional oversight mechanisms to ensure the Board is accountable.

Why Codify the Vulnerabilities Equities Process (VEP)?

- Balance two national security interests: the need to collect important, actionable intelligence and the need to patch vulnerabilities in technology products used by American consumers and businesses.
- Bring transparency to the process by making public the aggregate number of zero day vulnerabilities discovered, aggregate number of vulnerabilities disclosed, and length of time kept before disclosure.
- Ensure continuation of the process regardless of Administration.
- Increase confidence in the VEP, could serve as model for nations around world.