

# United States Senate

WASHINGTON, DC 20510

October 24, 2016

The President  
The White House  
1600 Pennsylvania Avenue, NW  
Washington, DC 20500

Dear Mr. President:

Given the growing threat to our nation's networks and digital services, we write to urge you to work with us to establish enduring government policies for the discovery, review, and sharing of security vulnerabilities.

The recent intrusions into United States networks and the controversy surrounding the Federal Bureau of Investigation's efforts to access the iPhone used in the San Bernardino attacks have underscored for us the need to establish more robust and accountable policies regarding security vulnerabilities. Specifically, we are exploring whether legislation is needed to establish government-wide policies with respect to two lines of effort: "bug bounty" programs that would help secure government networks like those used by the Office of Personnel Management, and formalizing the vulnerabilities equities process, which notifies software and hardware manufacturers of vulnerabilities discovered in their products.

**Bug Bounty Programs:** The private sector has been using bug bounty programs for decades to reward people who report security vulnerabilities in companies' applications, websites, and networks. Earlier this year, the Department of Defense launched "Hack the Pentagon," the first cyber bug bounty program in the history of the federal government. Of the 1,410 vetted U.S.-based hackers who registered for the Pentagon's program, 250 successfully found vulnerabilities and 138 submissions were found to be "legitimate, unique and eligible for a bounty."

We believe such programs represent a cost-effective way to supplement and support the people who defend our government's IT systems – and these efforts should not be limited to the Pentagon's networks. As such, we request that your administration work with us to establish standards and appropriate coordination platforms to build on the success of the Department's pilot and promote government-wide bug bounty programs.

**Vulnerabilities Equities Process (VEP):** Over the last several years, your administration, led by White House Cybersecurity Coordinator Michael Daniel, has made progress in establishing the VEP as the primary process for deciding whether a government entity must disclose to private companies' information about security vulnerabilities in their products, or whether the government may withhold the information for law enforcement or intelligence purposes. We believe the VEP framework is vital to ensuring that security vulnerabilities are either disclosed immediately so the relevant companies can strengthen consumer security, or put through a robust, accountable, and expeditious review process in the exceptional circumstances when the government may wish to delay disclosure for a limited amount of time.


During a Senate Armed Services Committee hearing on September 13<sup>th</sup>, Admiral Rogers said the NSA has utilized a “vulnerability evaluation process” since 2014 and that its “overall disclosure rate [of vulnerabilities to companies] has been 93 percent or so.” However, as of today, there is no legal obligation on government agencies to report the security vulnerabilities they discover or acquire to the White House-led VEP, nor is the VEP codified in law. In fact, it is unclear to us if all security vulnerabilities acquired by our government currently go through the VEP.

Therefore, we request that your administration work with us to establish comprehensive and enduring policies governing the VEP process, including standard criteria for reporting vulnerabilities to the VEP, guidelines for making VEP determinations, clear time limits for each stage of the process, adequate participation of all relevant government agencies, and regular reporting to Congress.

Finally, last year Congress passed, and you signed, the Cybersecurity Information Sharing Act of 2015 (CISA). We were early proponents of this legislation, which directs the federal government to increase its sharing of cyber information with the private sector to assist companies in protecting their systems, and provides clear authority and liability protection for private sector entities to share information with the government. We encourage your administration to use all of the authorities available under CISA to make progress on the lines of effort we have outlined above.

Thank you for your attention to these important issues. We look forward to working closely with your administration on these vital national security challenges in the weeks ahead.

Sincerely,



Angus S. King, Jr.  
United States Senator



Martin T. Heinrich  
United States Senator