SHADOW BROKERS GETS RESULTS! CONGRESS FINALLY MOVES TO OVERSEE VULNERABILITIES EQUITIES PROCESS

Since the Snowden leaks, there has been a big debate about the Vulnerabilities Equities Process — the process by which NSA reviews vulnerabilities it finds in code and decides whether to tell the maker or instead to turn it into an exploit to use to spy on US targets. That debate got more heated after Shadow Brokers started leaking exploits all over the web, ultimately leading to the global WannaCry attack (the NotPetya attack also included an NSA exploit, but mostly for show).

In the wake of the WannaCry attack, Microsoft President Brad Smith wrote a post demanding that governments stop stockpiling vulnerabilities.

> Finally, this attack provides yet another example of why the stockpiling of vulnerabilities by governments is such a problem. This is an emerging pattern in 2017. We have seen vulnerabilities stored by the CIA show up on WikiLeaks, and now this vulnerability stolen from the NSA has affected customers around the world. Repeatedly, exploits in the hands of governments have leaked into the public domain and caused widespread damage. An equivalent scenario with conventional weapons would be the U.S. military having some of its Tomahawk missiles stolen. And this most recent attack represents a completely unintended but disconcerting link between the two most serious forms of cybersecurity threats

> in the world today — nation-state action and organized criminal action.
>
> The governments of the world should treat this attack as a wake-up call. They need to take a different approach and adhere in cyberspace to the same rules applied to weapons in the physical world. We need governments to consider the damage to civilians that comes from hoarding these vulnerabilities and the use of these exploits. This is one reason we called in February for a new "Digital Geneva Convention" to govern these issues, including a new requirement for governments to report vulnerabilities to vendors, rather than stockpile, sell, or exploit them.

But ultimately, the VEP was a black box the Executive Branch conducted, without any clear oversight.

The Intelligence Authorization would change that. Starting 3 months after passage of the Intel Authorization, it would require each intelligence agency to report to Congress the "process and criteria" that agency uses to decide whether to submit a vulnerability for review; the reports would be unclassified, with a classified annex.

In addition, each year the Director of National Intelligence would have to submit a classified list tracking what happened with the vulnerabilities reviewed in the previous year. In addition to showing how many weren't disclosed, it would also require the DNI to track what happened to the vulnerabilities that were disclosed. One concern among spooks is that vendors don't actually fix their vulnerabilities in timely fashion, so disclosing them may not make end users any safer.

There would be an unclassified report on the aggregate reporting of vulnerabilities both at the government level and by vendor. Arguably,

this is far more transparency than the government provides right now on actual spying.

This report would, at the very least, provide real data about what actually happens with the VEP and may show (as some spooks complain) that vendors won't actually fix vulnerabilities that get disclosed. My guess is SSCI's mandate for unclassified reporting by vendor is meant to embarrass those (potentially including Microsoft?) that take too long to fix their vulnerabilities.

I'm curious how the IC will respond to this (especially ODNI, which under James Clapper had squawked mightily about new reports). I also find it curious that Rick Ledgett wrote his straw man post complaining that Shadow Brokers would lead people to reconsider VEP after this bill was voted out of the SSCI; was that a preemptive strike against a reasonable requirement?

SEC. 604. REPORTS ON THE VULNERABILITIES EQUITIES POLICY AND PROCESS OF THE FEDERAL GOVERNMENT.

Report Policy And Process.—

(1) IN GENERAL.—Not later than 90 days after the date of the enactment of this Act and not later than 30 days after any substantive change in policy, the head of each element of the intelligence community shall submit to the congressional intelligence committees a report detailing the process and criteria the head uses for determining whether to submit a vulnerability for review under the vulnerabilities equities policy and process of the Federal Government.

(2) FORM.—Each report submitted under paragraph (1) shall be submitted in unclassified form, but may include a classified annex.

(b) Annual Report On Vulnerabilities.—

(1) IN GENERAL.—Not less frequently than once

each year, the Director of National Intelligence shall submit to the congressional intelligence committees a report on—

(A) how many vulnerabilities the intelligence community has submitted for review during the previous calendar year;

(B) how many of such vulnerabilities were ultimately disclosed to the vendor responsible for correcting the vulnerability during the previous calendar year; and

(C) vulnerabilities disclosed since the previous report that have either—

(i) been patched or mitigated by the responsible vendor; or

(ii) have not been patched or mitigated by the responsible vendor and more than 180 days have elapsed since the vulnerability was disclosed.

(2) CONTENTS.—Each report submitted under paragraph (1) shall include the following:

(A) The date the vulnerability was disclosed to the responsible vendor.

(B) The date the patch or mitigation for the vulnerability was made publicly available by the responsible vendor.

(C) An unclassified appendix that includes—

(i) a top-line summary of the aggregate number of vulnerabilities disclosed to vendors, how many have been patched, and the average time between disclosure of the vulnerability and the patching of the vulnerability; and

(ii) the aggregate number of vulnerabilities disclosed to each responsible vendor, delineated by the amount of time required to patch or mitigate the vulnerability, as defined by thirty day increments.

(3) FORM.—Each report submitted under paragraph (1) shall be in classified form.

(c) Vulnerabilities Equities Policy And Process

Of The Federal Government Defined.—In this section, the term “vulnerabilities equities policy and process of the Federal Government” means the policy and process established by the National Security Council for the Federal Government, or successor set of policies and processes, establishing policy and responsibilities for disseminating information about vulnerabilities discovered by the Federal Government or its contractors, or disclosed to the Federal Government by the private sector in government off-the-shelf (GOTS), commercial off-the-shelf (COTS), or other commercial information technology or industrial control products or systems (including both hardware and software).