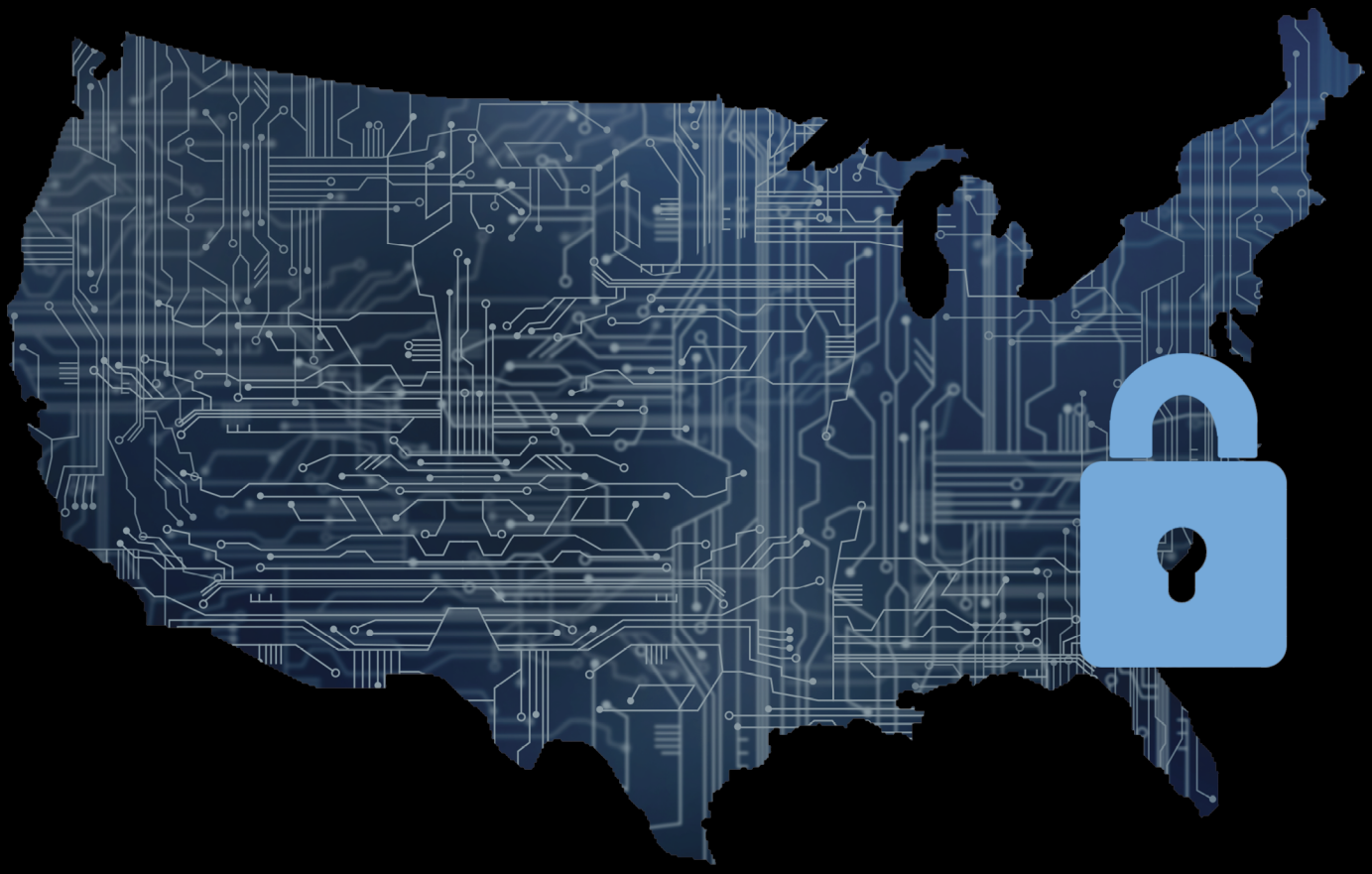
Columbia | SIPA
Journal of International Affairs
November 2016

The U.S. Government and Zero-Day Vulnerabilities

From Pre-Heartbleed to Shadow Brokers

JASON HEALEY



In August 2016, a group calling itself Shadow Brokers released a cache of top secret cyber spying capabilities almost certainly belonging to the U.S. National Security Agency (NSA). Out of the fifteen exploits in the cache, several appear to be previously unknown vulnerabilities (a so-called zero day or 0day vulnerability).[1] Worryingly, these vulnerabilities were in security products produced by Cisco, Juniper, and Fortinet, each widely used to protect U.S. companies and critical infrastructure, as well as other systems worldwide. As of this writing, the Shadow Brokers are still revealing new vulnerabilities and there may be more zero days discovered.

The existence of these capabilities begs many questions critical to the future of cyberspace:

1. Should the NSA have told vendors like Cisco about these vulnerabilities?
2. What is the process for determining whether to retain or disclose them to vendors?
3. Do these revelations mean this process is broken?
4. How many does the U.S. government retain every year?
5. How big is the U.S. arsenal of such capabilities?
6. What should be done next?

This report, based on research over the past six months from Jason Healey, senior research scholar at Columbia University's School of International and Public Affairs (SIPA) and a class of graduate students, provides the best current answers for these questions.

Based on numerous interviews and the U.S. government's own public statements about its policies, the NSA almost certainly should have disclosed these vulnerabilities to Cisco, Juniper, and Fortinet (just as the Federal Bureau of Investigation (FBI) should have told Apple about the vulnerability it used in April 2016 to access the iPhone of the San Bernardino murderers).[2] In January 2014, President Obama made it government policy to disclose by default any new vulnerability. If any agency wants to keep a zero day, they have to argue their case through the Vulnerability Equities Process (VEP) to an Equities Review Board chaired by the National Security Council (NSC) and attended by representatives from other agencies, including those most concerned with the security of critical U.S. infrastructure like the Department of Homeland Security (DHS) and the Department of Commerce. According to participants interviewed, this process is conducted at senior levels, and participants meet quite regularly.

The president and his NSC staff were quite clear in their criteria: in general, a vulnerability should be disclosed and if the vulnerability represents a particularly high risk or is widespread in U.S. critical infrastructure, the decision should tilt even further toward disclosure. The NSA bug in a Cisco security product certainly qualifies as widespread use. However, there are important loopholes to this policy and by keeping the Cisco, Juniper, and Fortinet vulnerabilities, NSA was probably not in direct violation of the president's policy. But the act of retaining these capabilities almost certainly violated the president's intent. The best case for the NSA retaining the Cisco vulnerability is that it had a mitigation plan, such as monitoring signals intelligence or other sources for signs that others

knew about it. If the agency discovered that these vulnerabilities were being used by others, it could then inform Cisco and Fortinet.

Every year the government only keeps a very small number of zero days, probably only single digits.

Although this evidence is not strong enough to indicate the VEP is hopelessly broken, it does appear to be in need of further strengthening. After all, the estimate we made before the Shadow Brokers' revelation is that every year the government only keeps a very small number of zero days, probably only single digits. Further, we estimate that the government probably retains a small arsenal of dozens of such zero days, far fewer than the hundreds or thousands that many experts have estimated. It appears the U.S. government adds to that arsenal only by drips and drabs, perhaps by single digits every year. The revelations coming from the Shadow Brokers' release may change these estimates, but so far have not.

However, before President Obama "reinvigorated" the VEP in January 2014, the NSA probably kept many more (likely dozens a year). In those days, the NSA largely made its own decisions, without having to consult with other parts of the government. It is worth noting, the exploits released by the Shadow Brokers were all from 2013 and would not have gone through the current White House-driven process.

Even so, the loss of trust in the White House process, the NSA, and the U.S. government's cyber efforts more generally has been monumental. At the very least the president needs to strengthen the process to close the apparent loopholes used by the NSA and FBI and improve transparency. The Shadow Brokers' revelation gives the impression that the NSA is operating on the extreme. In fact, the VEP is a good process for a critical function, reviewing when the government will retain or disclose vulnerabilities. The White House and the NSA should act quickly and transparently to retain th trust of American technologists, the U.S. public, and its allies.

Keep It or Patch It? The U.S. Vulnerability Equities Program

The U.S. government has used vulnerabilities and their associated exploits offensively since at least the 1990s, but until 2010 there was no process for sharing this knowledge between agencies or for working out the various equities between offensive and defensive mandates.[3] During the early 2000s, the NSA developed a strong internal process based on intelligence gain and loss tradeoffs, but there was no formal external or government-wide involvement. The decision to retain or disclose a particular vulnerability lay directly with the director of the NSA.

In the earlier days of signals intelligence, U.S. adversaries like the Soviet Union used their own communications technologies, so there were no significant tradeoffs involved. Breaking them for

intelligence purposes did not put U.S. companies or infrastructure at risk. That all changed with the Internet and advent of a (mostly) borderless cyberspace with everyone using similar or identical technologies.

The modern U.S. Vulnerability Equities Process began in 2008 when President Bush ordered, in the Comprehensive National Cybersecurity Initiative, for the U.S government to develop a "joint plan" for dealing with offensive cyber capabilities and specifically called for a "Vulnerabilities Equities Process."[4] This led in 2010 to the promulgation of a formal policy by the Office of the Director of National Intelligence.[5] The VEP is just part of a far larger ecosystem of vulnerability and disclosure, described in a recent report by New America, a U.S. think tank.[6] This ecosystem includes security researchers who find new vulnerabilities, vendors who patch them and perhaps seek them out through a corporate or independent "bug bounty" program, grey markets and other intermediaries who help broker connecting researchers to vendors (to patch) or attackers (to gain illicit entry), and government agencies that are sometimes attackers and sometimes defenders.

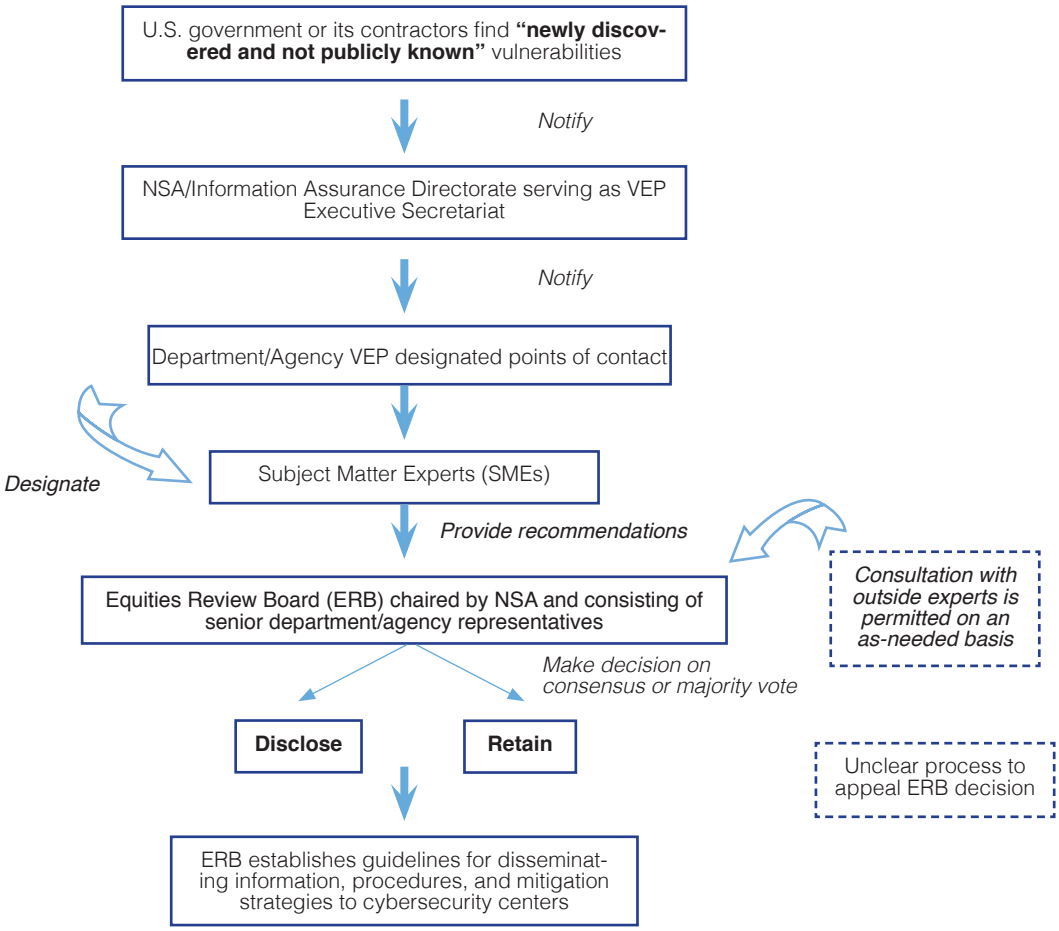
Within the United States, there are two general categories of government stakeholders in this process: those that use vulnerabilities and their associated exploits for offensive purposes and those whose equities are on the defensive side and are tasked with protecting U.S. infrastructure. The Department of Defense, the intelligence community, and law enforcement agencies all have elements that utilize vulnerabilities and exploits for one purpose or another. Each agency has its own process for determining its internal equities before presenting them to the interagency process. The Department of Commerce, the Department of Treasury, the Department of Energy, and the Department of Homeland Security are on the defensive side, looking to best secure cyberspace and the critical infrastructure sectors they oversee (though the law enforcement agencies within DHS mean the department can sometimes be conflicted).

Taking Shape

In 2008, a working group convened by the secretaries of state, defense, and homeland security, the attorney general, and the director of national intelligence (DNI) developed a joint plan to improve the U.S. government's offensive and defensive capabilities "to better defend information systems."[7] This plan recommended, among other things, the development of a Vulnerabilities Equity Process, for the purpose of "codifying and systematizing the U.S. government's handling of zero-day exploits."[8] Between 2008 and 2009, a group led by the Office of the Directorate of National Intelligence (ODNI) implemented this recommendation with a policy titled, "Commercial and Government Information Technology and Industrial Control Product or System Vulnerabilities Equities Policy and Process," one of a series of redacted documents released as part of a request under the Freedom of Information Act and subsequent lawsuit by the Electronic Frontier Foundation. This ODNI policy set out processes for notification, decision making, and appeals, and established an

executive secretariat role within the NSA (see Figure 1).[9]

Figure 1. VEP Process 2010 to 2014



A critical new element of this policy was that even though the process was run by the NSA there was a role for the "interagency," the other departments that had a stake in whether or not to disclose or retain vulnerabilities. Now DHS and other defensive agencies had a seat at the table, including the Equities Review Board (ERB), which would make the final decision. Just as importantly, in bureaucratic circles there was now a process to appeal ERB decisions, though the details have been redacted by ODNI.

The new policy applies to all parts of the U.S. government and its contractors. While the focus has remained largely on the NSA, the Central Intelligence Agency (CIA) and FBI also use vulnerabilities. The policy also includes all vulnerabilities (hardware or software) that were "newly discovered and not publicly known," regardless of whether they were discovered by the government or purchased on the grey markets, which sell to governments and other hacking groups. However, in a notable loophole, agencies did not have to submit vulnerabilities that were not "newly discovered." That is, if the zero day was discovered prior to 2010, they could be retained with no subsequent review. Indeed, once a vulnerability went through the process and was retained there was no periodic

review to see if the decision was still solid risk management. Also, this process would have excluded non-commercial vulnerabilities and probably those that were not made or used in the United States or by its allies. If the CIA or NSA were able to get their hands on a zero day in a Russian-made S-400 air defense missile system, they would not need DHS concurrence to keep it secret.

More practically, in the August 2016 Shadow Brokers' release of NSA capabilities, there were several vulnerabilities in a Chinese-made firewall by TopSec.[10] These may not need to go through the VEP process as they are not widely used in the United States. Even the computer security community, in the collective response to the revelations, focused on the U.S. products, indicating this risk management decision by the government may be the correct one. There has also been little fuss over vulnerabilities in an older Cisco product, the Pix firewall. It may be a zero day, but one that is in a product so obsolete that Cisco will not even fix it.[11] Cisco of course says it should have been informed anyhow, but for the Pix and TopSec examples it is understandable why they pose little risk and, in any process that balances foreign espionage and U.S. cybersecurity, they would be retained.

And it does appear the VEP is part of a relatively mature process. According to Admiral Michael Rogers, now director of NSA (DIRNSA), in his 2014 confirmation testimony to the Senate Armed Services Committee, in this review process "technical experts document the vulnerability in full classified detail, options to mitigate the vulnerability, and a proposal for how to disclose it … when NSA decides to withhold a vulnerability for purposes of foreign intelligence … [we] will attempt to find other ways to mitigate the risks to national security systems and other US systems."[12]

The default position of this process was "to disclose vulnerabilities in products and systems used by the US and its allies," and in fact the "NSA has always employed this principle in the adjudication of vulnerability findings," according to the Senate testimony by Admiral Rogers. In an email exchange with the research team, former DIRNSA General Michael Hayden agreed with the proviso that it was "consistent with my experience [and] NEVER taken lightly. Might have previously, trended toward offense … but always taken seriously and fulcrum [towards defense] shifted over time."[13] The NSA was more likely to keep a vulnerability if it was considered to be NOBUS—so obscure or complex it is "not usable by anyone but us."[14] However, there was significant doubt in the technology community and media. The suspicion was that "the government seemed to maintain the following policy: when it discovered or purchased a vulnerability, the default was not to disclose the vulnerability to affected companies, instead stockpiling the vulnerability for later use and leaving citizen and industry users vulnerable."[15]

As it turns out, according to a former NSC staffer, in the years after 2010, "VEP was dormant. NSA continued to run their own internal process but did not formally include outside agencies."[16] As we will see in the next section, even President Obama's own cyber coordinator felt the policy had to be "reinvigorated" in 2014.[17]

In the meantime, the VEP came under much more focused criticism in the wake of documents re-

leased by Edward Snowden. President Obama commissioned the Review Group on Intelligence and Communications Technologies whose December 2013 report examined the extent of NSA programs and called for dozens of urgent and practical reforms.[18] Regarding vulnerabilities, it recommended:

- "The National Security Council staff should manage an interagency process to review on a regular basis the activities of the US Government regarding attacks that exploit a previously unknown vulnerability in a computer application or system."

- "US policy should generally move to ensure that Zero Days are quickly blocked, so that the underlying vulnerabilities are patched on US Government and other networks. In rare instances, US policy may briefly authorize using a Zero Day for high priority intelligence collection, following senior, interagency review involving all appropriate departments."

In January 2014, President Obama accepted the recommendations of the Commission, instituting a new policy, or a "reinvigoration" as it has since been called. However, this was still entirely classified so the first indications of the new policy became public only months later.

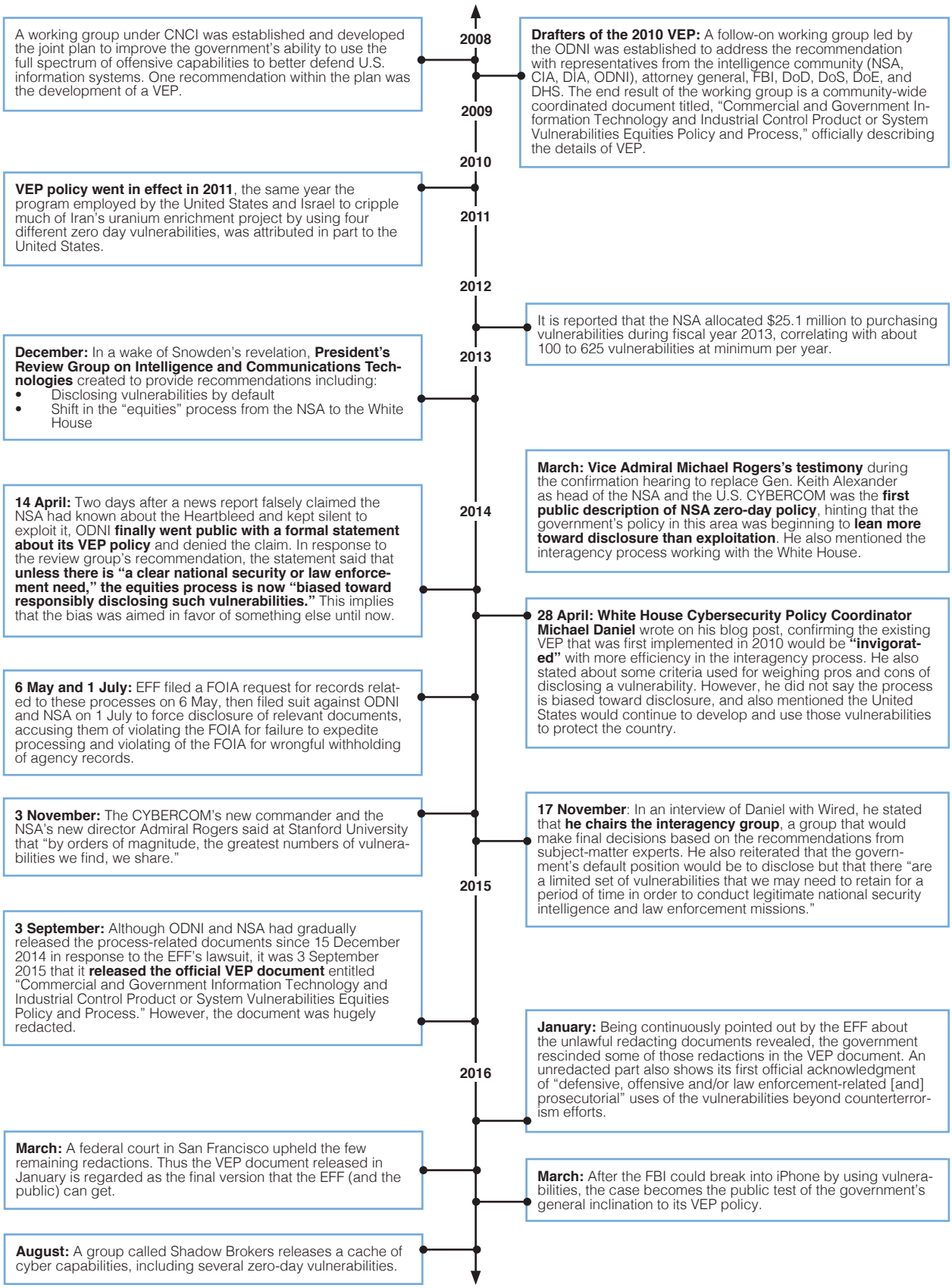
On 11 March 2014, during his confirmation hearings to become director of the NSA and commander of U.S. Cyber Command, Vice Admiral Michael S. Rogers echoed the call for increased interagency management of the process. Admiral Rogers confirmed that the NSA and White House were working to "put into place an interagency process for adjudication of 0-day vulnerabilities."[19] Rogers also for the first time revealed the default policy for discovered zero days would be to "disclose vulnerabilities in products and systems used by the US and its allies." In another new revelation, Rogers revealed that the interagency proposal mandated that the NSA collaborate with other government stakeholders like U.S. Cyber Command, the Defense Information Systems Agency, and DHS to discuss risk mitigation whenever they decided to retain a vulnerability for their own use.

Coming in the wake of so many stunning revelations of NSA surveillance programs, the vulnerability disclosure process did not gain too much of a spotlight. Merely one month later, however, details about the Heartbleed bug drew public attention and criticism.

The Influence of Heartbleed

In April 2014, a new vulnerability, dubbed Heartbleed, exploded onto the security scene. The Heartbleed bug is a serious vulnerability in the common OpenSSL cryptographic software library that allows anyone exploiting it to steal information normally protected by the encryption layer that is used to secure Internet commerce and other important functions. In the days immediately after the bug was announced by a private security firm, Bloomberg news reported that the NSA "knew for at least two years" about the flaw and "regularly used it to gather critical intelligence."[20] Heartbleed is one of the most serious flaws discovered in the history of the Internet. If indeed the NSA had known about

Figure 2. Timeline of VEP Policy



the vulnerability and had failed to disclose it to the vendors, it would seem that all of the rhetoric about preserving security being the primary policy of the government was disingenuous.

Just a day after the Bloomberg story, however, veteran national security (and increasingly cyber) journalist David Sanger published his own story about Heartbleed in the *New York Times* that questioned whether the NSA did indeed have knowledge of Heartbleed before it was publicly divulged.[21] Sanger's story promoted a formal denial from the White House that the government knew about Heartbleed. Likewise, the ODNI published on its blog that "reports that NSA or any other part of the government were aware of the so-called Heartbleed vulnerability before April 2014 are wrong. The Federal government was not aware of the recently identified vulnerability in OpenSSL until it was made public in a private sector cybersecurity report."[22] Sanger's article also prompted a statement by the NSC confirming the statement by Admiral Rogers that the "process is biased toward responsibly disclosing such vulnerabilities."[23]

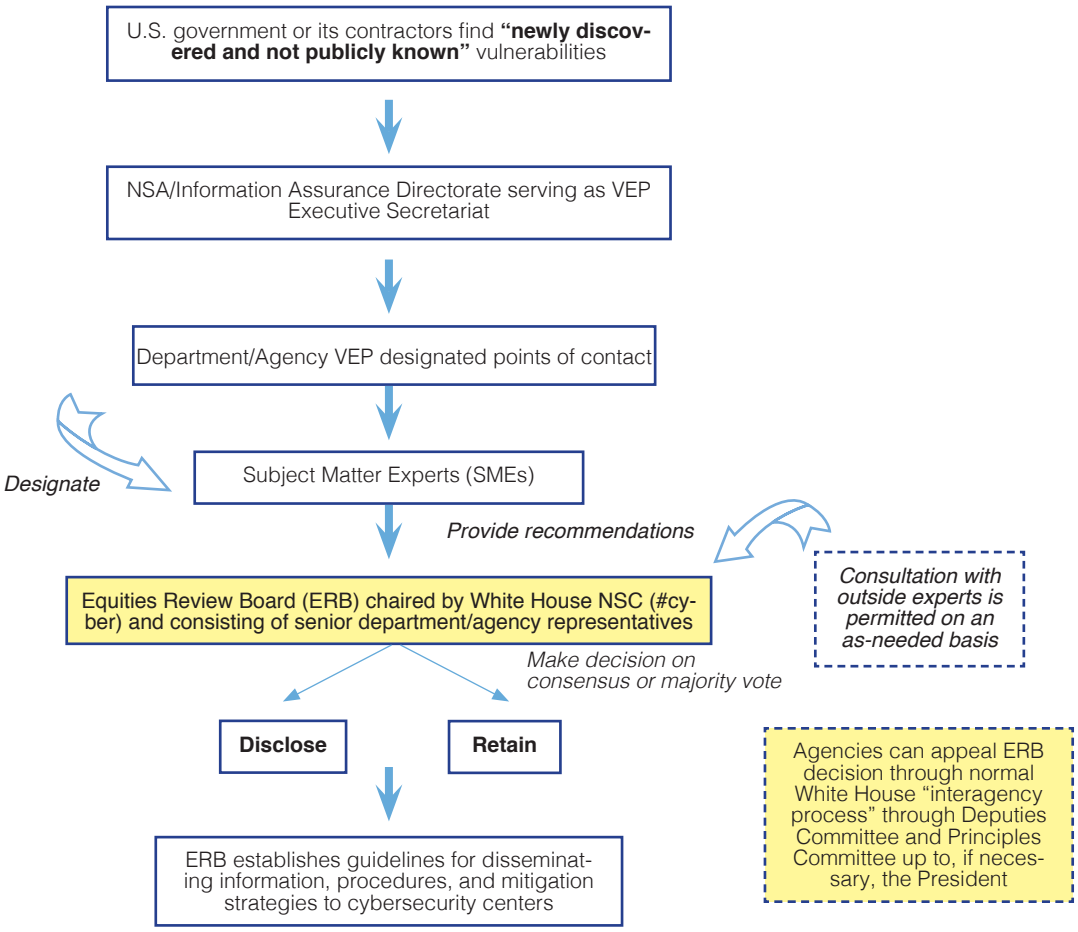
Following Sanger's article and the many others that followed, Michael Daniel, the special assistant to the president and the cybersecurity coordinator at the NSC, gave additional details on the White House's blog that was an unparalleled amount of transparency on an issue of signals intelligence collection. Daniel reiterated the intelligence community's statements that it was not aware of the "identified Heartbleed vulnerability until it was made public,"[24] a significant public statement and the first instance the government had publicly acknowledged whether or not it had a technical vulnerability in its arsenal. Daniel also provided the startlingly reasonable set of criteria that the NSC version of the ERB would use in its deliberations to retain or disclose vulnerabilities:

1. How much is the vulnerable system used in the core Internet infrastructure, in other critical infrastructure systems, in the U.S. economy, and/or in national security systems?
2. Does the vulnerability, if left unpatched, impose significant risk?
3. How much harm could an adversary nation or criminal group do with knowledge of this vulnerability?
4. How likely is it that we would know if someone else was exploiting it?
5. How badly do we need the intelligence we think we can get from exploiting the vulnerability?
6. Are there other ways we can get it?
7. Could we utilize the vulnerability for a short period of time before we disclose it?
8. How likely is it that someone else will discover the vulnerability?
9. Can the vulnerability be patched or otherwise mitigated?

Echoing statements from other policymakers,[25] Daniel also highlighted the recent changes in U.S. policy regarding how vulnerabilities are handled. According to Daniel, the U.S. government had "re-

invigorated … their … efforts to implement existing policy with respect to disclosing vulnerabilities" and outlined nine key criteria that would be used to determine whether or not to disclose a vulnerability that had been discovered.[26]

Figure 3. "Reinvigorated" VEP Process 2014 -



Daniel further elaborated in an interview with Kim Zetter of *Wired* magazine that the proper interagency communications had not taken place to ensure that the correct amount of visibility was maintained across all government entities. While subject matter experts may have been informed, coordination and integration with various agency agendas did not exist. This interagency communication was to be "reinvigorated" to ensure that it happened as "consistently and as thoroughly" as was outlined in the policy.[27] To ensure that this process was being properly implemented, the White House would also be taking control of the decision-making process (see Figure 3). Instead of an ERB run by the NSA, Daniel himself would chair the board, which would be centered at the National Security Council. The NSA, though still the executive agent for the VEP, was now out of the business of deciding for itself whether or not to report the vulnerabilities it discovered.

There was one other major revelation. In the fall of 2015, the NSA asserted that historically it "dis-

closed 91 percent of vulnerabilities discovered in products that have gone through our internal review process and that are made or used in the United States."[28] It said at the time that the remaining 9 percent were "either fixed by vendors before we notified them or not disclosed for national security reasons."

This admission by the NSA was noteworthy for several reasons. It was not prompted by a scandal, unlike so many of the other releases of information coming after Heartbleed or Snowden. The NSA also seems to imply the true number would actually have been higher than 91 percent but the vendor patched the vulnerabilities first. Any products not "made or used in the United States" (and assumedly close allies, such as the "Five-Eye" partners of the United Kingdom, Australia, Canada, and New Zealand) were excluded from this count, which suggests that perhaps the government keeps all such vulnerabilities or has some other process.

Subsequently, in October 2016, a senior NSA official clarified that the small percent of retained vulnerabilities also did not include vulnerabilities they deemed "trivial," such as if they had no real security impact, or if the vulnerability was in "outdated" software that was no longer updated by the vendor.[29] So, if the NSA finds a vulnerability in Windows NT, it may not notify Microsoft. Ford Motors would not issue a recall if it found a security defect in an old Model T car and Microsoft no longer patches any vulnerabilities in NT, which is now considered obsolete.

Dozens, Hundreds, or Thousands? Analysis and Assessment

The VEP process and decision criteria that have been made public seem to be, in public policy terms, a relatively mature and thoughtful process. According to many people we interviewed for our zero-day research, participants in the equities review process are senior members of the administration (including several deputy assistant or assistant secretaries) and meet frequently at various seniority levels. Especially compared to other White House committees that meet lackadaisically based on other priorities, it's an active bureaucratic process.

Still, there are several aspects of the today's VEP that remain unclear:

1. How many vulnerabilities does the U.S. government retain every year?
2. How big is the U.S. arsenal of such capabilities?
3. Should the NSA have told Cisco and Fortinet about these firewall vulnerabilities? Shouldn't the FBI have told Apple about the vulnerability it purchased in April?
4. Do these revelations mean this process is broken?
5. What should be done next?

Our best estimate, with moderate confidence, is that prior to the 2014 "reinvigorated" policy the U.S. government retained dozens of vulnerabilities per year. This assessment covers only vulnerabilities in U.S.

or allied systems and is based on several lines of evidence and assumptions, most importantly that the 91 percent figure for the amount of vulnerabilities the NSA has historically disclosed is roughly accurate.

There are some reasons to believe an estimate of dozens disclosed per year may be either too high or too low. It is possible, but not probable, that this estimate undershoots and that the number is a bit higher, in the low hundreds. The argument for "too low" is rooted in part to suspicion about whether the assertion that NSA officials disclose 91 percent can be trusted, but also the news from the Shadow Brokers' release that just in this single cache of firewall exploits the NSA had three zero days. If there are similar caches for other security products (for routers, for mobile devices, and for different operating systems) then perhaps the number retained per year will climb.

In support of "too high," or "about right," Dickie George, formerly technical director of the NSA's Information Assurance Directorate (the defensive side of the NSA) has said retaining vulnerabilities was "very rare."[30] Former NSA director Michael Hayden supported this sentiment.[31] Moreover, Symantec reports having discovered only one to two dozen zero days "in the wild" per year.[32] By comparison, there is about 10,000 total vulnerabilities appearing in the Open Source Vulnerability Database.[33]

The most convincing line of evidence was based on reports from the Snowden documents of the NSA's budget of $25.1 million for "additional covert purchases of software vulnerabilities."[34] Table 1 examines two estimates of how much such a budget might purchase and what that would mean for the overall number retained every year. It would be somewhere between 50 and 250 vulnerabilities per year. We assume the NSA would also have discovered, not bought, a similar number of vulnerabilities, while the FBI and CIA would have purchased about the same amount.

Table 1

Simple Estimate	More Realistic Estimate
Purchases: • 250 x important vulnerabilities in commercial software used or made in the United States or allies @ $100k each of which 91% disclosed ~25 total of vulnerabilities purchased per year are retained	Purchases: • 12 critical vulnerabilities in commercial systems used or made in the United States or allies @ $1 million • 2 critical vulnerabilities in non-commercial (such as Russian weapon systems) @ $1 million • 6 critical vulnerabilities in non-U.S. systems (such as Chinese-made router) @ $500k • 32 major vulnerabilities at $250k • 44 total commercial vulnerabilities of which 91% disclosed ~5 total of vulnerabilities purchased per year are retained
Assume similar number purchased by other agencies and similar number discovered internally = 25 x 3	Assume similar number purchased by other agencies and similar number discovered internally = 5 x 15
Total retained: ~75 *Even with margin of error of 3x, only ~225 retained*	Total retained: ~15 *Even with margin of error of 3x, only ~45 retained*

Lacking conflicting evidence, we believe our estimate is accurate, but of course further information—such as a release of far more zero-day vulnerabilities by the Shadow Brokers—might revise this assessment upwards.

This assessment is entirely for the process prior to 2014, for which there is admittedly limited evidence. For the period of the new White House "reinvigorated" policy, there is far more information available.

We estimate with high confidence that in the period from 2014 to today, the U.S. government retains single-digit numbers of vulnerabilities per year. One of the most compelling pieces of evidence is leaked information from the White House. In 2016, there were reports that in one year (probably 2015), the U.S. government kept "only about two [vulnerabilities] for offensive purposes out of about 100 the White House reviewed" as part of the VEP.[35] A former NSC staffer involved in the VEP process subsequently pointed to that statistic in his own articles, which almost surely went through NSC review. When someone with first-hand knowledge points to such information, it is a good (but not perfect) sign that the answer is believed to be correct.

Moreover, in 2015 there were only dozens of zero days discovered "in the wild" (one count by Symantec resulted in 54[36] while another by veteran vulnerability researcher Brian Martin resulted in 40, due to different counting methods).[37] This makes a number in the single digits seem reasonable. If the NSA was keeping dozens or hundreds (and a similar number was kept by the Chinese and Russian military and intelligence agencies, plus organized crime, plus Iran and North Korea, etc.) then it seems that far more than 50 would be discovered.[38]

The final key section of analysis was the total number of vulnerabilities retained by the U.S. government. If it had been keeping perhaps dozens per year and now single digits, what can that flow tell us about the total size? Though all these terms are probably improper comparisons, is it analogized as a "horde," "arsenal," or merely a "weapons locker" of capabilities?

We estimate with moderate confidence that the current U.S. arsenal of zero-day vulnerabilities is probably in the dozens. The arsenal is a function of several factors, an equation through which it is difficult to get much higher than 50 or 60. The factors include how many years the United States has been retaining zero days (at least fifteen), how many are retained per year (dozens before 2014 and single digits since), the average number burned per year (say 50 percent), the average life of a zero day once used (approximately 300 days[39]), the average number of zero days discovered by vendors or used by other actors which thereby renders them useless for the United States (25 percent), and the average half-life of a zero-day vulnerability if not used (approximately 12 months). Note that this count critically depends on the "single digit per year" assessment discussed above. This count does not include battlefield and non-commercial systems, non-U.S. systems (such as the TopSec firewall vulnerabilities in the Shadow Brokers' release), or U.S. government exploits that utilize vulnerabilities that have already been made public.

This assessment is supported by comments from White House Cyber Coordinator Michael Daniel who is on record saying that "the idea that we have these vast stockpiles of vulnerabilities stored up—you know, *Raiders of the Lost Ark* style—is just not accurate."[40] This is very loose support so the research team looked for other ways to possibly disprove this estimate. One way was suggested in a conversation with Jeff Moss, founder of the Black Hat and DEF CON conventions, who mentioned the NSA Tailored Access Operations capabilities book released by Snowden at the end of 2013. This book, advertised by the media as the "NSA toolbox" or a mail-order catalog, contained only 50 cyber capabilities, in the middle range of our estimates of "dozens."[41]

Issues and Recommendations

While it is clear that the attention from the president and his NSC has indeed reinvigorated the process, there are instances that indicate it still may not be functioning as President Obama intended (or the technology sector expects). Privacy and security experts like Chris Soghoian of the American Civil Liberties Union have been particularly harsh commentators on these issues.

The FBI's recent purchase of a tool to unlock the iPhone 5C raises questions regarding when an agency needs to report a vulnerability to the VEP. According to the former deputy director of the NSA, Chris Inglis, this should have been submitted to the NSC ERB for review, because of the "tension between individual and collective security … equities process should be run to put both on a level playing field."[42] If it did get submitted by the FBI, "neither they nor the US government as a whole must tell Apple about how they did it. But if they follow the White House's own policy, it appears they should."[43]

In this case, the FBI found a loophole, purchasing only the use of a tool based on a vulnerability unknown to Apple, but not the rights to (or apparently understanding of) the actual zero day itself. Any effort to get this knowledge was prohibited by a non-disclosure agreement signed by the FBI as part of its contract to have access to the vulnerability. According to FBI Director Comey, this decision was made to save money, intimating that more in-depth knowledge would have been even more expensive than the reported six figures the bureau spent. Because the FBI had so little understanding of how the tool worked, officials determined that there would be no point to undertake a government review.[44] If allowed to continue, this loophole could allow law enforcement and intelligence agencies to bypass the president's intent. Purchase any exploit through this process and you will not have to (or not be able to) report the issue to the vendor, even if such a vulnerability is critical to the U.S. society or economy.

The more recent disclosure from the group calling itself the Shadow Brokers is potentially more worrisome, as it contained several zero days. Based on the criteria detailed by the NSC's Daniel in 2014, these seem to have been natural candidates to disclose to the vendors. Cisco and Fortinet are both

U.S. companies, their products are widely used in the "US economy," including "critical infrastructure systems," and they are security products, so clearly the vulnerabilities fit the criteria for "harm" and "significant risk." These vulnerabilities were developed as early as 2013, when the NSA ran the process itself with little outside influence. It is possible these even predated the first VEP guidance in 2010, meaning they were grandfathered in with no review necessary, ever.

Perhaps the expected intelligence gain from these vulnerabilities was so high, the NSA felt the risk was worth taking, especially if that risk could be mitigated by monitoring signals intelligence for signs Russia or China had found the vulnerabilities and only then disclosing them to Cisco and Fortinet. Perhaps the vulnerabilities were so obscure that the NSA felt safe using them. This judgment is possibly supported by the fact that in three years they still had not been publicly discovered.

The existence of two vulnerabilities is hardly evidence of hoarding.

There has been far less concern over several vulnerabilities in TopSec firewalls. As that company is Chinese and their products are infrequently used, if at all, in the United States or its allies, the risk to the U.S. economy and infrastructure would have been low, but the potential intelligence value was quite high.

The discovery of two new zero-day vulnerabilities in this cache has led to intense discussion in the cybersecurity community, much of it saying the VEP is broken or that the NSA "hoards" vulnerabilities.[45] For now, we stand by the estimates from our research. The existence of two vulnerabilities is hardly evidence of hoarding. Even if this cache is only 2 percent of the NSA's total arsenal, then that means they only have 100 zero days, a number still within, though near the higher end of, our estimated range. A "hoard" implies perhaps more than 1,000 zero-day vulnerabilities ready for action; it is far from obvious that revelations of two firewall zero days hints at numbers that high.

The criticism that the "VEP is toothless" is actually relatively benign compared to other criticisms, often from former intelligence officers that the VEP was either too strong or worse than useless. For example, a former analyst for the Defense Intelligence Agency, Mike Tanji, wrote that intelligence agencies should not "place the security of the Internet—and commercial concerns that use it—above their actual missions."[46] Dave Aitel and Matt Tait took this point even farther, saying the VEP is pointless because there is "no clear evidence that Russian and Chinese operational zero-days overlap with those" used by U.S. intelligence.[47] Giving up this rich intelligence source, therefore, does not stop U.S. adversaries as they have a completely different toolkit of vulnerabilities.

It might not be the job of those particular agencies to care about the security of the Internet and U.S. commercial concerns, but these objectives have been a stated priority for the last three administrations back to 1998. The VEP is a process for the political level to balance that against other priorities of national and economic security. As long as it wants to simultaneously secure the Internet and use it as a tool against its adversaries, the White House needs an interagency process to achieve that

balance. As expressed by Chris Inglis, the most recent former NSA deputy director, in an interview with us, the VEP is not just about maximizing NSA efficiency—the argument that "if only we could take the shackles off we could do great things"—but rather the opposite, checking its power relative to other priorities, about "checks and balances."[48] Moreover, no matter how good the NSA is, "we are not the smartest guys on the planet," and even if it were true that there is limited overlap between U.S. and adversary tool sets, fewer bugs are better and the country is clearly stronger with a process for determining what to keep and what to release, for policy balance.

Recommendations

The Shadow Brokers still have more exploits to release so the U.S. government—and especially the NSA—will have to respond to a lot more uncomfortable revelations. The NSC must start now to get ahead of that process. The government let over two weeks (and still counting as far of this writing) pass before making any comment, ceding the headlines and news cycles. The NSC spokesperson should be ready for the next set of revelations with a prepared statement along these lines:

> "We will neither confirm nor deny these were U.S. government cyber capabilities. But the president has set the policy that we will tell companies by default when we discover vulnerabilities in their products. Because this is such a critical issue, the president centralized decision power in the White House rather than at the NSA.
>
> "The president's cyber coordinator has outlined the criteria to make the decision to disclose or retain and some of our internal processes to do so. The director of the NSA has testified that when we retain such vulnerabilities we have a mitigation plan. We stand by all of these statements.
>
> "However, we will review the Vulnerabilities Equities Process to improve its effectiveness and transparency in order to continue to earn the trust of America's citizens, our world-leading technology sector, and Internet users around the world."

The FBI's iPhone loophole and the Shadow Brokers' revelations give the impression of a process out of control, discrediting the VEP. Our assessment is that it is an excellent process, but clearly needs improvements in effectiveness and transparency. In fact, the lack of trust is so severe that the NSC should probably replace the name "Vulnerability Equities Process" with something less tied to the NSA, like the "Vulnerability Disclosure Review."

Former NSC officials Rob Knake and Ari Schwartz have provided an excellent set of recommendations that should be the starting point of any reform.[49] Currently, the VEP is only a policy, if one driven by the White House. It should be formalized as an executive order to elevate its standing (and possibly increase the chances that it will be inherited by following administrations). In addition, right now vulnerability reviews are "one and done." Once the decision is made to retain a vulnerability, an agency can keep using it forever, even if the risk changes significantly. A periodic review, say every

year or two, can correct for this, as well as work through the vulnerabilities discovered before 2010 that were exempted from review.

Knake and Schwartz also recommend transferring the role of the VEP executive secretary function from the NSA to the more defensively minded DHS, along with more transparency through an annual public report. In the current version of the VEP there appears to be little independent oversight, and there is room for a mandated congressional role and perhaps also for the Privacy and Civil Liberties Oversight Board or Office of Inspector General. Of course, a re-reinvigorated VEP should also close the loophole used by the FBI so agencies cannot bypass the VEP because of a non-disclosure agreement or other chicanery.

In addition to this list are some developed by the Columbia research team. The VEP should include a presidential mandate that agencies may not use discovered vulnerabilities until it has been approved for retention by the ERB to prevent agencies from bureaucratically delaying the process while they squeeze the orange dry. Moreover, the VEP system allows for opinions to be heard from government stakeholders, but does not include an active industry perspective. Including any active participants from companies in the field would obviously be problematic for competitive and security reasons, but there is a wealth of cleared (or clearable) retired industry experts and academics who could provide that perspective without risking the protection of methods or proper competition. Even if such experts cannot be included in the review and decision about retaining vulnerabilities, they can easily be included in a review to revamp the current VEP.

Quarterly and yearly statistics should be made public to improve transparency. This might include actual numbers reviewed and retained (as with the leaked information that the ERB reviewed 100 and only kept two), but at the very least the number of meetings and agencies represented could be made public with little national security risk. The executive secretariat already creates an annual report of VEP proceedings so a portion of this report should be released at the unclassified level. If the U.S. government released such information it could go a long way toward instilling faith in the process and help create the norm of how responsible states act when developing cyber programs.

Another important transparency initiative is for the NSA, and other agencies, to shed light on the risk mitigation plan when a vulnerability is retained. Admiral Rogers testified that they "attempt to find other ways to mitigate the risks." In the Shadow Brokers' case, subsequent news revealed that the NSA had known for three years that their tools had been compromised, yet did not tell Cisco. Instead the "NSA tuned its sensors to detect use of any of the tools by other parties, especially foreign adversaries with strong cyber espionage operations, such as China and Russia," and "because the sensors did not detect foreign spies or criminals using the tools on U.S. or allied targets, the NSA did not feel obligated to immediately warn the U.S. manufacturers."[50] This sounds exactly in line with what would be expected of the NSA risk management plan.

Yet, because this process is not well understood by those outside the VEP, it leads to the assumption

that U.S. companies have been left undefended because of excess secrecy, when in fact this might as easily show a successful risk mitigation plan because the NSA was still able to use the vulnerability and apparently no one else discovered it. Because the NSA is so tight lipped about the risk mitigation plan, technologists and commentators get to assume the worst. Of course, intelligence agencies won't want to spill sources and methods, but even an outline of the elements of a risk mitigation plan (monitoring for signatures in signals intelligence and within the U.S. government networks for instance) would help and would not expose significant capabilities to U.S. adversaries.

And as much as the United States gets grief when it becomes public that the NSA or FBI have retained vulnerabilities, it is the only nation with anything approaching this level of transparency. According to Jim Lewis of the Center for Strategic and International Studies, "perhaps 30 nations are acquiring offensive cyber capabilities; some would say many more."[51] Yet the U.S. VEP is the only review process that we know about. The silver medal goes to the United Kingdom, where the Government Communications Headquarters (the British equivalent of the NSA) announced as of late April that they had disclosed 20 vulnerabilities to vendors in 2016.[52] Other nations with offensive programs—including the Netherlands, Sweden, France, Germany, Australia, and Canada—should be as transparent as the United States and develop their own VEP-like structure.

The Open Technology Initiative at New America also proposes that the U.S. government investigates its participation in the zero-day market, support bug bounty programs so vendors can be the first to hear of vulnerabilities in their software, and other strong recommendations.[53]

Conclusion

Presidents should, of course, have the ability to use cyber capabilities to spy on U.S. adversaries, catch criminals, and fight terrorists. The current VEP is a reasonable balance—it's a process with presidential guidance to favor defense and run by the NSC. But as good as it is, the developments of 2016 show that it needs to grow. Cyberspace has just become too critical to the U.S. economy and society.

There are other benefits as well. Joe Nye, the veteran national security scholar, wrote in 2015 that,

> "[I]f the United States unilaterally adopted a norm of responsible disclosure of zero-days to companies and the public after a limited period, it would destroy their value as weapons — simultaneously disarming ourselves, other countries and criminals without ever having to negotiate a treaty or worry about verification. Other states might follow suit. In some aspects, cyber arms control could turn out to be easier than nuclear arms control."[54]

As our research has detailed, the United States actually has unilaterally adopted such a norm of responsible disclosure through the president's decision that the U.S. bias is to disclose zero days

to vendors. By doing so, it is not unilaterally disarming, as some fear, but taking arrows out of its adversaries' quivers. Unfortunately, the United States is squandering this opportunity by a lack of greater transparency, leading to a loss of confidence from the technology sector and cybersecurity community. Following our recommendations will not only improve the security of the United States and cyberspace as a whole, but also help to ensure a more peaceful cyberspace.

About the Research

This paper was made possible through support by the Global Policy Institute of Columbia University and the Carnegie Corporation of New York. Parts of this writing were based on research done for a course on policy dilemmas in cybersecurity taught by Jason Healey at SIPA. Those students divided into five teams to research multiple aspects of the government's role in vulnerabilities lifecycle.

- **Team 1**: Jackie Burns-Koven, Natasha Cohen, and Andrew Liu researched zero-day markets and government involvement.
- **Team 2**: Mellissa Zubaida Ahmed, Igor Bakharev, Robert Diamond, Nozomi Mizutani, Jittip Mongkolnachaiarunya, and Nicole Softness researched the U.S. government vulnerability disclosure program.
- **Team** 3: Arsla Jawaid, Laurence Kinsella, Andrew Pfender, and Arastoo Taslim researched security researchers and corporate vulnerability programs, such as responsible disclosure and bug bounty programs.
- **Team 4**: Niko Efstathiou, Daniel Ismael Gonzalez, Marie von Hafften, and Adriana Tache researched vulnerability databases and quant measurement.
- **Team 5**: Sherman Chu, Timothy Hodge, Caitlin LaCroix, Amine Moussaoui, and Anthony Sanford researched the actual use of zero days in the wild and whether other nations have explicit zero-day policies.

Jason Healey is responsible for the content of this report. He is a senior research scholar at Columbia University's School of International and Public Affairs and senior fellow at the Atlantic Council. Follow him on Twitter @Jason_Healey.

Endnotes

[1] David Sanger, "Obama Lets N.S.A. Exploit Some Internet Flaws, Officials Say," *New York Times*, 12 April 2014.
[2] Jason Healey, "Why the FBI will eventually reveal its iPhone hack to Apple," *Christian Science Monitor*, 25 March 2016.
[3] Tom Gjelten, "In Cyberwar, Software Flaws Are A Hot Commodity," NPR *Morning Edition*, 12 February 2013.
[4] For a more complete account, see Ari Schwartz and Rob Knake, "Government's Role in Vulnerability Disclosure," Belfer Center, June 2016.
[5] "Vulnerabilities Equities Process Highlights," Electronic Frontier Foundation, 2015.
[6] Andi Wilson, Ross Schulman, Kevin Bankston, and Trey Herr, "Bugs in the System." New America, July 2016.
[7] "Vulnerabilities Equities Process Highlights," 2015.
[8] "Exhibit C: Classified Declaration of James B. Richberg, Office of the Director of National Intelligence." Electronic Frontier Foundation, 2016.
[9] "Exhibit B: Commercial and Government Information Technology and Industrial Control Product or System Vulnerabilities Equities Policy and Process," Electronic Frontier Foundation, 2010.
[10] "Equation Group Firewall Operations Catalogue," 2016.
[11] Omar Santos, "The Shadow Brokers EPICBANANA and EXTRABACON Exploits," Cisco Blogs, 17 August 2016.
[12] Michael Rogers, "Advance Questions for Vice Admiral Michael S. Rogers, USN," Senate Armed Services Committee, 11 March 2014.
[13] Michael Hayden, email message to author, July 2016.
[14] Andrea Peterson, "Why everyone is left less secure when the NSA doesn't help fix security flaws," *Washington Post*, 4 October 2013.
[15] Mailyn Fidler, "Anarchy or Regulation: Controlling the Global Trade in Zero-Day Vulnerabilities," Stanford University, 2014.
[16] Former White House official, email message to author, July 2016.
[17] Kim Zetter, "U.S. Gov Insists It Doesn't Sotckpile Zero-Day Exploits to Hack Enemies," *Wired*, 17 November 2014.
[18] Review Group on Intelligence and Communications Technologies, "Liberty and Security in a Changing World," 12 December 2013.
[19] Rogers, 2014.
[20] Michael Riley, "NSA Said to Have Used Heartbleed Bug, Exposing Consumers," Bloomberg, 12 April 2014.
[21] Sanger, 2014.
[22] ODNI Public Affairs Office, "Statement on Bloomberg News story that NSA knew about the 'Heartbleed bug' flaw and regularly used it to gather critical intelligence," *IC on the Record*, 11 April 2014.
[23] Sanger, 2014.
[24] National Security Agency/Central Security Service, Twitter post, 11 April 2014.
[25] Sanger, 2014.
[26] Michael Daniel, "Heartbleed: Understanding When We Disclose Cyber Vulnerabilities," White House Blog, 28 April 2014.
[27] Zetter, 2014.
[28] National Security Agency/Central Security Service, "Discovering IT Problems, Developing Solutions, Sharing Expertise," 30 October 2015.
[29] Off-the-record conversation with author and senior NSA official, 20 October 2016.
[30] Sean Sposito, "NSA reveals hundreds of bugs a year, says former official." *San Francisco Chronicle*, 5 May 2016.
[31] Michael Hayden in discussion with author, 2016.
[32] Symantec Corporation, "A New Zero-Day Vulnerability Discovered Every Week in 2015," 2015.
[33] Brian Martin, email message to Adriane Tache, 6 April 2016.
[34] Brian Fung, "The NSA hacks other countries by buying millions of dollars' worth of computer vulnerabilities," *Washington Post*, 31 August 2013.
[35] Chris Strohm, Jordan Robertson, and Michael Riley, "Thank You for Hacking IPhone, Now Tell Apple How You Did It," Bloomberg, 22 March 2016.
[36] Symantec Corporation, "Internet Security Report, Volume 21," April 2016.
[37] Brian Martin, email message to author, 29 April 2016.
[38] Ibid.
[39] Leyla Bilge and Tudor Dumitras, "Before We Knew It: An Empirical Study of Zero-Day Attacks In The Real World" (proceedings, ACM Conference on Computer and Communications Security, New York, NY, 2012, 833-844).
[40] Zetter, 2014.
[41] Jacob Appelbaum, Judith Horchert, and Christian Stöcker, "Shopping for Spy Gear: Catalog Advertises NSA Toolbox," *Der Spiegel*, 29 December 2013.
[42] Strohm, 2016.
[43] Healey, 2016.
[44] Oscar Raymundo, "It's official: FBI won't share its secret iPhone hack with Apple," *MacWorld*, 27 April 2016.
[45] Andy Greenberg, "The Shadow Brokers Mess Is What Happens When the NSA Hoards Zero-Days," *Wired*, 17 August 2016.

[46] Michael Tanji, "Intelligence Agencies Are Not Here to Defend Your Enterprise," Linkedin, 19 April 2016.
[47] Dave Aitel and Matt Tait, "Everything You Know About the Vulnerability Equities Process Is Wrong," *Lawfare*, 18 August 2016.
[48] Chris Inglis in discussion with author, 23 August 2016.
[49] Ari Schwartz and Rob Knake, "Government's Role in Vulnerability Disclosure," Belfer Center, June 2016.
[50] Joseph Menn and John Walcott, "Exclusive: Probe of leaked U.S. NSA hacking tools examines operative," Reuters, 22 September 2016.
[51] James Andrew Lewis, "The Rationale for Offensive Cyber Capabilities," *Strategist*, 8 June 2016.
[52] Joseph Cox, "GCHQ Has Disclosed Over 20 Vulnerabilities This Year, Including Ones in iOS," *Motherboard*, 29 April 2016.
[53] Wilson, Schulman, Bankston, and Herr, 2016.
[54] Joseph Nye, "The world needs new norms on cyberwarfare," *Washington Post*, 1 October 2015.

JIA.SIPA.COLUMBIA.EDU