Journal of Law & Commerce
Vol. 42, No. 1 (2023) ● ISSN: 2164-7984 (online)
DOI 10.5195/jlc.2023.270 ● http://jlc.law.pitt.edu

NOTES

RECALIBRATING THE USE OF ZERO-DAY VULNERABILITIES

Kellen Carleton

NOTES

RECALIBRATING THE USE OF ZERO-DAY VULNERABILITIES

Kellen Carleton[*]

I. INTRODUCTION

The United States Government has a significant interest in the market for zero-day vulnerabilities. In addition to nearly every sector of critical infrastructure, many governments around the world rely on a relatively small amount of software systems that are not fully secured.[1] These software systems are intricate, complex, and contain countless vulnerabilities that are unknown even to the software's developers.[2] These unknown vulnerabilities are commonly referred to as a "zero-day."[3] Hackers around the world, whether employed by a legitimate government agency or a black-market criminal organization, have an interest in finding zero-day vulnerabilities in software systems and developing exploits to leverage those vulnerabilities to gain information.[4] Zero-day exploits can be used to gain entry into an adversary's systems, sometimes undetected, and then wreak havoc at the

[*] Kellen Carleton is a 2024 Graduate of the University of Pittsburgh School of Law. Previously, he received his M.S. in International Relations and Politics in 2019, and his B.S. in Public Policy and Management in 2018, both from Carnegie Mellon University.

[1] Office of the Press Secretary, Presidential Policy Directive—Critical Infrastructure Security and Resilience, THE WHITE HOUSE PRESIDENT BARACK OBAMA (Feb. 12, 2013), https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil [hereinafter PPD-21].

[2] Mailyn Fidler, *Regulating the Zero-Day Vulnerability Trade: A Preliminary Analysis*, 11.2 I/S: J.L. & POL'Y FOR INFO. SOC'Y 405, 408 (2015).

[3] *Id.* at 406.

[4] *Id.*

Vol. 42, No. 1 (2023) ● ISSN: 2164-7984 (online) ● ISSN 0733-2491 (print)
DOI 10.5195/jlc.2023.270 ● http://jlc.law.pitt.edu

most opportune time.[5] Because the modern global economy relies on technology and the power of computing, the security of those software systems has become paramount, and the vulnerabilities have become very valuable.[6] Similarly, government intelligence services and black-market hackers alike have realized that vulnerabilities in technology have become a gold mine for intelligence gathering.[7]

The U.S. Government is uniquely situated as both a customer in the zero-day market, and as an entity responsible for protecting against zero-day vulnerabilities. Many of the companies that develop widely used software platforms are American companies that serve a global audience.[8] Without a doubt, the U.S. Government has an interest in helping to protect these companies from foreign adversaries that wish to do the United States harm.[9] However, intelligence agencies also have an interest in finding and exploiting software vulnerabilities to spy on terrorist groups, adversaries, and nations considered both friendly and adversarial to the United States.[10]

As the zero-day market has rapidly exploded, the U.S. Government needed a way to balance these competing interests; helping to secure and protect software systems that are widely used by American companies and the American people, and exploiting unknown vulnerabilities for the purposes of gaining intelligence.[11] To do that, the executive branch drew up a process by which they would weigh all concerns about what to do with a vulnerability found in a vendor's software, and whether they would disclose the vulnerability to the vendor or restrict the vulnerability for use by

---

[5] *Id.* at 408–09.

[6] EXEC. OFF. OF THE PRESIDENT, NATIONAL CYBERSECURITY STRATEGY (Mar. 2, 2023), https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf [hereinafter National Cybersecurity Strategy].

[7] Michael Daniel, *Heartbleed: Understanding When We Disclose Cyber Vulnerabilities*, THE WHITE HOUSE PRESIDENT BARRACK OBAMA (Apr. 28, 2014, 3:00 PM), http://www.whitehouse.gov/blog/2014/04/28/heartbleed-understanding-when-we-disclose-cyber-vulnerabilities.

[8] STEFAN FREI, NSS LABS, THE KNOWN UNKNOWNS: EMPIRICAL ANALYSIS OF PUBLICLY KNOWN SECURITY VULNERABILITIES 1 (2013).

[9] Daniel, *supra* note 7.

[10] NICOLE PERLROTH, THIS IS HOW THEY TELL ME THE WORLD ENDS: THE CYBERWEAPONS ARMS RACE 107–08 (Bloomsbury Publishing, 2021).

[11] Daniel, *supra* note 7.

Vol. 42, No. 1 (2023) ● ISSN: 2164-7984 (online) ● ISSN 0733-2491 (print)
DOI 10.5195/jlc.2023.270 ● http://jlc.law.pitt.edu

intelligence agencies.[12] This process is known as the Vulnerabilities Equities Process (VEP).

This Note examines the current VEP and offers solutions to recalibrate the decision-making process for the Intelligence Community by assessing the legal foundations of the VEP, current proposed reforms, and other recommendations for ensuring that the process is producing unbiased decisions that take into account the goals and interests of both the public and private sectors.

II. BACKGROUND INFORMATION ON THE VULNERABILITIES EQUITIES PROCESS

A. Creation of the VEP by the Bush Administration in 2008

The VEP traces its origins to National Security Presidential Directive-54 (NSPD-54), also known as Homeland Security Presidential Directive-23 (HSPD-23). NSPD-54/HSPD-23 was a directive from the George W. Bush administration, dated January 8, 2008, which was designed to "establish United States policy, strategy, guidelines, and implementation actions to secure cyberspace."[13] Further, NSPD-54/HSPD-23 was aimed at "improv[ing] the Nation's security against the full spectrum of cyber threats and in particular, the capability of the United States to deter, prevent, detect, characterize, attribute, monitor, interdict, and otherwise protect against unauthorized access to National Security Systems, federal systems, and private-sector critical infrastructure systems."[14]

It is clear from this directive that even in 2008, the U.S. Government was at least beginning to grasp the importance of "maintain[ing] unrestricted access to . . . cyberspace for a broad range of national purposes."[15] While

---

[12] Exec. Office of the President, Vulnerabilities Equities Policy and Process for the United States Government, TRUMP WHITE HOUSE (2017), https://trumpwhitehouse.archives.gov/sites/whitehouse.gov/files/images/External%20-%20Unclassified%20VEP%20Charter%20FINAL.PDF [hereinafter VEP Charter].

[13] EXEC. OFF. OF THE PRESIDENT HSPD-54/HSP-23, NATIONAL SECURITY PRESIDENTIAL DIRECTIVE/HOMELAND SECURITY PRESIDENTIAL DIRECTIVE 1 (2008), https://fas.org/irp/offdocs/nspd/nspd-54.pdf [hereinafter NSPD-54/HSPD-23].

[14] NSPD-54/HSPD-23, *supra* note 13, at 1.

[15] *Id.* at 2.

Vol. 42, No. 1 (2023) ● ISSN: 2164-7984 (online) ● ISSN 0733-2491 (print)
DOI 10.5195/jlc.2023.270 ● http://jlc.law.pitt.edu

hacking and cybercrime had not yet risen to the current threat level, the U.S. Government understood that cybercrime had the ability to be significantly disruptive and was costing American businesses upwards of tens of billions of dollars annually.[16]

The VEP was disclosed to the public in 2014 in a White House blog post by Michael Daniel who was at the time the Special Assistant to the President and Cybersecurity Coordinator.[17] Daniel released details about the Executive Branch "re-invigorating efforts to implement existing policy with respect to disclosing vulnerabilities" in the wake of the Heartbleed vulnerability.[18] While Daniel did not identify the policy by name, the details of the blog post clearly refer to the VEP, as is evidenced by the list of considerations that are weighed by decision-makers, many of which also appear in Annex B of the VEP Charter.[19]

While it is unknown exactly when the VEP was created and implemented, the VEP Charter was officially unclassified and released in 2017.[20] The charter specifically cites Paragraph 49 of NSPD-54/HSPD-23, which states that "the Secretaries of State, Defense, and Homeland Security, the Attorney General, and the Director of National Intelligence (DNI) shall submit . . . a joint plan for the coordination and application of offensive capabilities to defend U.S. Information Systems."[21] Further, Paragraph 49 stated that the plan shall be submitted to the Assistant to the President for National Security Affairs and the Assistant to the President for Homeland Security and Counterterrorism.[22] Paragraph 53(e) of NSPD-54/HSPD-23 is also of note, as it establishes that the directive "shall be implemented in a manner to ensure that the privacy rights and other legal rights of Americans are recognized."[23] The foundations of what would become the current VEP are important in later sections, where reforms are discussed to ensure that the

[16] *Id.*
[17] Daniel, *supra* note 7.
[18] *Id.*
[19] *Id.*
[20] Andi Wilson Thompson, *Assessing the Vulnerabilities Equities Process, Three Years After the VEP Charter*, LAWFARE BLOG (Mar. 30, 2023, 5:53 PM), https://www.lawfareblog.com/assessing-vulnerabilities-equities-process-three-years-after-vep-charter.
[21] NSPD-54/HSPD-23, *supra* note 13, ¶ 49.
[22] *Id.* at ¶ 49.
[23] *Id.* at ¶ 53.

Vol. 42, No. 1 (2023) ● ISSN: 2164-7984 (online) ● ISSN 0733-2491 (print)
DOI 10.5195/jlc.2023.270 ● http://jlc.law.pitt.edu

VEP is in line with its legal foundations and the guiding principles set out in NSPD-54/HSPD-23.

B. The VEP's Current Structure and Membership

As stated above, an unclassified version of the VEP was released in 2017.[24] The general purpose of the VEP is to set out considerations that are to be weighed by the government when deciding whether to disseminate vulnerability information to the vendor/supplier in the expectation that it will be patched.[25] Alternatively, the government could temporarily restrict the knowledge of the vulnerability to relevant government entities so that it can be used for national security and/or law enforcement purposes, such as intelligence collection, military operations, or counterintelligence.[26]

The VEP's principal decision makers constitute the Equities Review Board (ERB), which has representatives from the following government agencies: Office of Management and Budget (OMB), Office of the Director of National Intelligence (ODNI), Department of the Treasury (TREAS), Department of State (DOS), Department of Justice (DOJ),[27] Department of Homeland Security (DHS),[28] Department of Energy (DOE), Department of Defense (DoD), Department of Commerce (DOC), and the Central Intelligence Agency (CIA).[29] The Charter provides that other executive agencies may be included in the decision-making process as needed.[30] The diversity of representation on the Board reflects the significant coordination and collaboration that is needed across agencies and industries to ensure

[24] VEP Charter, *supra* note 12, at 1.

[25] *Id.*

[26] *Id.*

[27] Representatives from the Department of Justice include representation of the Federal Bureau of Investigation (FBI) and the National Cyber Investigative Joint Task Force (NCIJTF).

[28] Representatives from the Department of Homeland Security include the National Cybersecurity Communications and Integration Center (NCCIC) and the United States Secret Service (USSS). It should be noted here that at the time of release of this VEP Charter, the Cybersecurity and Infrastructure Security Agency (CISA) had not yet been established. It is likely that at least one of DHS' representatives to the VEP is the Director of CISA or their designee.

[29] VEP Charter, *supra* note 12, at 3–4.

[30] *Id.*

Vol. 42, No. 1 (2023) ● ISSN: 2164-7984 (online) ● ISSN 0733-2491 (print)
DOI 10.5195/jlc.2023.270 ● http://jlc.law.pitt.edu

careful and deliberate decisions are made. The Charter notes that the ERB would meet monthly, or sooner as needed.[31]

The ERB meets monthly and is led by the "VEP Director" who is "the Special Assistant to the President and Cybersecurity Coordinator, or an equivalent successor."[32] The second-in-command is the VEP Executive Secretariat who "facilitates information flow, discussions, determinations, documentation, and recordkeeping for the process."[33] The VEP Executive Secretariat currently sits within the NSA.[34] To ensure that decisions are made in an unbiased fashion, the process is coordinated by the National Security Council. This prevents any individual agency from holding too much power when determining how a vulnerability is dealt with.

Further, Section 5 of the VEP Charter lays out the decision-making process. First, there is an initial threshold that must be met for a vulnerability to enter the process. This threshold only requires that a vulnerability be (1) newly discovered, and (2) not publicly known.[35] Section 5.2.4 then lays out dissemination options designed to be methodical and predictable to the members of the ERB. All decisions are to be made in "full consultation with all concerned agencies" and be based on "repeatable techniques or methodologies that enable benefits and risks to be objectively evaluated by VEP Participants."[36]

C. VEP Annex B "Equity Considerations"

Perhaps the most interesting section of this release of the VEP is Annex B, which lays out considerations that the ERB must take into account when deciding to disclose or restrict a vulnerability.[37] The considerations are broadly split into two categories: (1) Defensive Equity Considerations, and

---

[31] *Id.* at 3.

[32] Since the creation of this document, there has been a new role established in the Executive Office of the President known as the National Cyber Director, a position that was established by the NDAA for Fiscal Year 2021 and on the recommendation of the Cyberspace Solarium Commission. The National Cyber Director is appointed by the President and confirmed by the Senate and is the President's principal advisor on cybersecurity policy and strategy.

[33] VEP Charter, *supra* note 12, at 5.

[34] *Id.* at 4.

[35] *Id.* at 5.

[36] *Id.* at 7.

[37] *Id.* at 13–14.

Vol. 42, No. 1 (2023) ● ISSN: 2164-7984 (online) ● ISSN 0733-2491 (print)
DOI 10.5195/jlc.2023.270 ● http://jlc.law.pitt.edu

(2) Intelligence, Law Enforcement, and Operational Equity Considerations.[38] Some categories listed under Defensive Equity Considerations are specific questions about the details and sophistication of the vulnerability, the various ways in which the vulnerability could be used to cause harm, how widespread the impact would be on U.S. interests, and what a potential mitigation might look like.[39] On the other side, there are considerations that ask similar questions but from a different perspective. More "offensive" minded considerations surround the value of the vulnerability, the types of information that can be obtained through the vulnerability, whether alternative means exist to obtain the targeted information, and potential impacts to private sector and international community partners.[40]

III. THE ZERO-DAY MARKET

As stated above, a zero-day vulnerability is "a software or hardware flaw for which there is no existing patch" and are commonly known in the information security community as "the most critical tool in a hacker's arsenal" which "offer[s] digital superpowers" that gives spies and cybercriminals alike a "cloak of invisibility."[41] Zero-day vulnerabilities can give hackers access to any company, government agency, or bank that relies on the affected software or hardware.[42]

The evolution of the market for zero-day vulnerabilities has its roots in the Cold War and the race between the United States and the Soviet Union for intelligence.[43] Zero-days can really be viewed as an outgrowth of normal intelligence gathering operations that were commonplace during the Cold War.[44] Former intelligence officials have stated that the NSA's insatiable desire to gain information at all costs during the Cold War and throughout the War on Terror has remained constant.[45] The intelligence community

[38] *Id.*
[39] *Id.*
[40] *Id.*
[41] PERLROTH, *supra* note 10, at 7.
[42] *Id.* at 8.
[43] Jason Healey, *The U.S. Government and Zero-Day Vulnerabilities: From Pre-Heartbleed to Shadow Brokers*, COLUM. J. INT'L AFFS. 2–3 (Nov. 1, 2016).
[44] *Id.*
[45] PERLROTH, *supra* note 10, at 100–10.

Vol. 42, No. 1 (2023) ● ISSN: 2164-7984 (online) ● ISSN 0733-2491 (print)
DOI 10.5195/jlc.2023.270 ● http://jlc.law.pitt.edu

remains determined to give their policymakers as much information as humanly possible in order to make the best decisions.[46]

While the mediums have changed dramatically and the impacts are felt in a more significant way, there has always been an attitude of aggressive intelligence collection.[47] The hunt for zero-day vulnerabilities is simply a change in the means by which the same intelligence gathering strategies persist.[48] The NSA and other intelligence agencies have devoted significant resources to finding zero-day vulnerabilities and developing exploits.[49] The NSA undertakes these activities because a small number of companies have created technology that is used widely throughout the world by both the public and private sectors. Companies such as Apple, Microsoft, Samsung, Alphabet (Google), IBM, Dell, Huawei (mostly in China), etc. provide the majority of the world's hardware and software.[50] While the cyber domain may seem like a vast ocean full of many unexplored areas, when the world economy and governments rely on a relatively small amount of technology, the attack surface suddenly does not seem so daunting and seems ripe for exploitation.

However, that proposition raises a serious moral hazard, especially for the U.S. Government. As the world became more reliant on digitization, the NSA was able to get unprecedented amounts of intelligence.[51] When the principal adversary of the United States was the Soviet Union, there were no tradeoffs involved,[52] as Americans spied on Russian technology while Russians backdoored American typewriters. However, the modern world was now using the same technologies—Microsoft operating systems, Oracle databases, Gmail, iPhones, and microprocessors—ubiquitously throughout daily life.[53] "Nobody seemed to be asking what all this breaking and entering

---

[46] *Id.* at 106.

[47] John M. Tidd, *From Revolution to Reform: A Brief History of U.S. Intelligence*, 28 SAIS REV. INT'L AFF. 5 (2008), https://www-jstor-org.pitt.idm.oclc.org/stable/pdf/27000112.pdf?refreqid=excelsior%3A14b658c814955296003ca2d56dcde57c&ab_segments=&origin=&initiator=&acceptTC=1.

[48] Healey, *supra* note 43, at 2.

[49] David E. Sanger, *Obama Lets N.S.A. Exploit Some Internet Flaws, Officials Say*, N.Y. TIMES, Apr. 12, 2014, https://www.nytimes.com/2014/04/13/us/politics/obama-lets-nsa-exploit-some-internet-flaws-officials-say.html.

[50] Fidler, *supra* note 2, at 408.

[51] PERLROTH, *supra* note 10, at 100.

[52] Healey, *supra* note 43, at 2–3.

[53] PERLROTH, *supra* note 10, at 114.

and digital exploitation might mean for the NSA's sponsors—the American taxpayers—who now relied on NSA-compromised technology not only for communication but for banking, commerce, transportation and health care."[54] Further, "nobody apparently stopped to ask whether in their zeal to poke a hole and implant themselves in the world's digital systems, they were rendering America's critical infrastructure . . . vulnerable to foreign attacks."[55]

In the midst of groundbreaking technological espionage accomplishments, the NSA never believed that these techniques could be used against the United States.[56] The NSA had an unrivaled hubris where they assumed, to the country's detriment, that all the flaws it was uncovering could not possibly be discovered by someone else.[57] While classic conceptions of the nuclear arms races were thought to be a thing of the past, the United States and its adversaries had now entered into a new arms race, and now they do not have an easy way out.[58]

Zero-day vulnerabilities exist in a couple of different types of markets.[59] There are legitimate markets in which large technology firms, government agencies, and private sector cybersecurity firms both develop and acquire zero-day vulnerabilities.[60] Companies such as Google,[61] Microsoft,[62] and Facebook[63] offer bounties, or payments, for bugs found in their software. The rewards can be rather lucrative, with rewards ranging from a couple of hundred dollars per vulnerability to nearly $150,000 for some bugs, depending on the bug.[64] There is also a significant black market trade for zero-day vulnerabilities that usually involves some aspect of criminal

---

[54] *Id.*
[55] *Id.* at 115.
[56] Fidler, *supra* note 2, at 412.
[57] *Id.*
[58] *Id.*
[59] *Id.* at 410.
[60] *Id.*
[61] GOOGLE BUG HUNTERS, *Google and Alphabet Vulnerability Reward (VRP) Rules*, https://bughunters.google.com/about/rules/6625378258649088/google-and-alphabet-vulnerability-reward-program-vrp-rules (last visited Sept. 21, 2023).
[62] MICROSOFT BUG BOUNTY PROGRAM, *Microsoft Security Response Center*, https://www.microsoft.com/en-us/msrc/bounty (last visited Sept. 21, 2023).
[63] FACEBOOK, *Meta Bug Bounty Program Info*, https://www.facebook.com/whitehat (last visited Sept. 21, 2023).
[64] Fidler, *supra* note 2, at 414.

Vol. 42, No. 1 (2023) ● ISSN: 2164-7984 (online) ● ISSN 0733-2491 (print)
DOI 10.5195/jlc.2023.270 ● http://jlc.law.pitt.edu

behavior, and is usually across borders.[65] Lastly, as described above, governments are also a significant buyer in the zero-day market, with the U.S. Government spending millions of dollars annually.[66]

IV. NEED FOR REFORM

The 2017 VEP Charter states the importance and the delicate nature of weighing vulnerability equities. The Charter articulates that these "vulnerabilities can have significant economic, privacy and national security implications when exploited."[67] The government is fully aware of both their own reliance on private sector software systems, as well as critical infrastructure's reliance on many of the same private sector software systems.[68] "Unpatched vulnerabilities leave not only U.S. Government (USG) systems, but also the systems of commercial industry and private citizens, vulnerable to intrusion."[69] In fact, the cost of cybercrime, due in no small part to zero-day vulnerabilities, is growing rapidly and is expected to hit nearly $10.5 trillion annually by 2025.[70]

There have been a few very visible examples of direct failures with the current VEP where vulnerabilities that were left unpatched were eventually exploited by China, Russia, and North Korea, among other adversaries.[71] Two of those examples are WannaCry and NotPetya, both exploiting the EternalBlue zero-day vulnerability in Microsoft software.[72]

---

[65] LILY ABLON ET AL., MARKETS FOR CYBERCRIME TOOLS AND STOLEN DATA: HACKERS' BAZAAR, 25, RAND Corp. (2014) (ebook), http://www.rand.org/pubs/research_reports/RR610.html.

[66] Barton Gellman & Ellen Nakashima, *U.S. Spy Agencies Mounted 231 Offensive Cyber Operations in 2011, Documents Show*, WASH. POST (Sept. 3, 2013), http://www.washingtonpost.com/world/national-security/us-spy-agencies-mounted-231-offensive-cyber-operations-in-2011-documents-show/2013/08/30/d090a6ae-119e-11e3-b4cb-fd7ce041d814_story.html.

[67] VEP Charter, *supra* note 12, at 1.

[68] *Id.*

[69] VEP Charter, *supra* note 12, at 2.

[70] Carmen Ene, *10.5 Trillion Reasons Why We Need A United Response To Cyber Risk*, FORBES, Feb. 22, 2023, https://www.forbes.com/sites/forbestechcouncil/2023/02/22/105-trillion-reasons-why-we-need-a-united-response-to-cyber-risk/?sh=7c74f28b3b0c.

[71] Perlroth & Shane, *In Baltimore and Beyond, a Stolen N.S.A. Tool Wreaks Havoc*, N.Y. TIMES (May 25, 2019), https://www.nytimes.com/2019/05/25/us/nsa-hacking-tool-baltimore.html.

[72] Ellen Nakishima, *NSA Officials Worried About the Day its potent hacking tool would get loose. Then it did*, WASH. POST (Mar. 16, 2017), https://www.washingtonpost.com/business/technology/nsa-officials-worried-about-the-day-its-potent-hacking-tool-would-get-loose-then-it-did/2017/05/16/50670b16-3978-11e7-a058-ddbb23c75d82_story.html.

The decision to restrict the EternalBlue zero-day was a product of the current VEP. EternalBlue was reportedly developed by the NSA after nearly one year of work, and it is said that EternalBlue produced significant intelligence and counterterrorism information.[73] However, in April 2017, the Shadow Brokers released EternalBlue as a part of a larger release of stolen NSA tools.[74] Within two months of the Shadow Brokers' release of EternalBlue, it was first used in the ransomware known as WannaCry, which is widely believed to have originated from North Korea.[75] WannaCry would go on to cripple the health system of Great Britain and was able to compromise critical healthcare systems.[76] Later, another ransomware known as NotPetya used the same EternalBlue vulnerability.[77] This time, the Russians tailored the NSA-developed weapon to wreak havoc all over the world, including significant damage throughout Ukraine.[78]

While not officially confirmed, it has been reported that the NSA possessed and was actively using the EternalBlue zero-day for nearly five years before it was ultimately stolen.[79] However, once it was stolen, it wreaked havoc and caused billions in damages for several U.S.-based companies.[80]

A. The VEP and the Public-Private Partnership on Cybersecurity

The VEP is a good microcosm for the tension that exists between the government and private companies with respect to cybersecurity. Companies

---

[73] Perlroth & Shane, *supra* note 71.

[74] Lily Hay Newman, *The Leaked NSA Spy Tool that Hacked the World*, WIRED (Mar. 7, 2018), https://www.wired.com/story/eternalblue-leaked-nsa-spy-tool-hacked-world/.

[75] *Id.*

[76] David E. Sanger, *U.S. Accuses North Korea of Mounting WannaCry Cyberattack*, N.Y. TIMES (Dec. 18, 2017), https://www.nytimes.com/2017/12/18/us/politics/us-north-korea-wannacry-cyberattack.html?searchResultPosition=4.

[77] Alex Hern, *WannaCry, NotPetya: How Ransomware Hit the Big Time in 2017*, THE GUARDIAN (Dec. 30, 2017), https://www.theguardian.com/technology/2017/dec/30/wannacry-petya-notpetya-ransomware.

[78] *Id.*

[79] Brad Smith, *The Need for Urgent Collective Action to Keep People Safe Online: Lessons from Last Week's Cyberattack*, MICROSOFT ON THE ISSUES (May 14, 2017), https://blogs.microsoft.com/on-the-issues/2017/05/14/need-urgent-collective-action-keep-people-safe-online-lessons-last-weeks-cyberattack/#sm.0000mpb068eggcqczh61fx32wtiui.

[80] Perlroth & Shane, *supra* note 71.

Vol. 42, No. 1 (2023) ● ISSN: 2164-7984 (online) ● ISSN 0733-2491 (print)
DOI 10.5195/jlc.2023.270 ● http://jlc.law.pitt.edu

such as Apple, Microsoft, Google, and Amazon own most of the products that are used throughout the government and critical infrastructure.[81] Not only do they produce the physical hardware, but they also develop all of the software systems. This means that the U.S. Government must work with their private sector partners to better defend cyberspace, including "enabling public-private collaboration at the speed and scale necessary" to properly defend critical infrastructure.[82]

The government does have some authority to regulate the private sector with respect to cybersecurity. While the Federal Trade Commission (FTC) has not engaged in any explicit rulemaking via the Administrative Procedures Act, the agency does have some power to regulate cybersecurity.[83] Specifically, the FTC can regulate "unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce" through Section 45(a)(1) of the FTC Act.[84] Further, through the Cybersecurity and Infrastructure Security Agency (CISA), the U.S. Government has significant roles in working with the private sector on cybersecurity best practices.[85] However, the U.S. Government deals with cybersecurity in a fragmented approach that operates in individual sectors and states rather than a federal-level cybersecurity or data security law.[86] Lastly, the government also has the power to force companies to improve their cybersecurity posture as a cost of doing business with government information.[87] However, these requirements are usually relatively low in order to not be too burdensome.

At the end of the day, it is the private sector's responsibility to secure their own networks and software systems. Current legislation and regulation does not sufficiently hold software vendors accountable for security flaws in

---

[81] Fidler, *supra* note 2, at 408.

[82] National Cybersecurity Strategy, *supra* note 6.

[83] *See* Federal Trade Commission Act, 15 U.S.C. §§ 41–58, 45(a)(1) (1914).

[84] 15 U.S.C. § 45 (1914).

[85] *See Cybersecurity Best Practices*, CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY, https://www.cisa.gov/topics/cybersecurity-best-practices.

[86] *See* DANIEL J. SOLOVE & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW 1011–14 (Wolters Kluwer, 7th ed. 2021).

[87] *See* The White House, EXEC. OFF. OF THE PRESIDENT, Executive Order on Improving the Nation's Cybersecurity, Subsection (h), (May 12, 2021), https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/.

Vol. 42, No. 1 (2023) ● ISSN: 2164-7984 (online) ● ISSN 0733-2491 (print)
DOI 10.5195/jlc.2023.270 ● http://jlc.law.pitt.edu

their products.[88] Private sector software products are used so pervasively throughout both the private and public sectors that they have become an integral part of everyday life.[89] Cyberattacks which expose software vulnerabilities are increasing in frequency and have become one of the most persistent economic and national security threats to the United States, causing tens of billions of dollars in damages annually.[90]

However, discussions about responsibilities in cybersecurity become complicated when there is proof that the U.S. Government is actively concealing vulnerabilities from the private sector that, in some cases, can lead to catastrophic cyber attacks that cause millions of dollars in damage.

V. CURRENT PROPOSED SOLUTIONS

The public and private sectors have distinct but similar goals. For both, the end goal is to have secure systems and to reduce harm from cyberattacks to the American people as much as possible. For the profit-seeking firms in the private sector, the goal is to reduce both the amount and impact of all types of cyber events for the purpose of maximizing profits and protecting their customers. On the flipside, the government's goal is to use all tools available to gain intelligence to give the necessary information to policymakers so they can make the most informed choices. These goals may at times seem to conflict, but there have been numerous efforts over the years to bring these parties closer together in a more collaborative working relationship. In fact, it is a key tenet of the Biden Administration's 2023 National Cybersecurity Strategy.[91]

The intelligence community plays "defense" in many different ways. One method of protection involves the use of offensive measures as a way to defend. This concept is known as "defend forward" or "persistent engagement," where the U.S. Government will actively pursue cyber threats and disrupt malicious cyber activity at the source rather than trying to

---

[88] Jane Chong, *Bad Code: The Whole Series*, LAWFARE BLOG (May 16, 2022, 3:27 PM), https://www.lawfareblog.com/bad-code-whole-series.

[89] Vincent R. Johnson, *Cybersecurity, Identity Theft, and the Limits of Tort Liability*, 57 S.C. L. REV. 255, 256 (2005).

[90] Chong, *supra* note 88.

[91] National Cybersecurity Strategy, *supra* note 6, at Strategic Objective 1.2 (p. 10).

actively repel threats as they come.[92] After all, many have heard the adage that "the best defense is a good offense."[93] After years of constantly playing from behind, the Trump Administration empowered U.S. Cyber Command to take a more offensive approach when it comes to defending America in cyberspace.[94] This includes a more aggressive approach when it comes to the handling of zero-day vulnerabilities.[95]

A. The PATCH Act

Currently, there is a current proposal to codify the current VEP before Congress called the PATCH Act.[96] The purpose of the "Protecting Our Ability to Counter Hacking" (PATCH) Act of 2017 is "to add transparency and accountability to the U.S. Government process for retaining or disclosing vulnerabilities in technology products, services, applications, and systems."[97] The PATCH Act codifies the current VEP and amends it slightly by having the Department of Homeland Security chair the Equities Review Board, not the aforementioned "VEP Director" that sits within the NSA.[98]

The PATCH Act also prescribes permanent membership on the Equities Review Board for the Director of the FBI, the Director of National Intelligence, the Director of the CIA, the Director of the NSA, and the Secretary of Commerce.[99] Ad hoc members would include the Secretary of State, the Secretary of the Treasury, the Secretary of Energy, a designee of the Federal Trade Commission, and also allows any member of the National

---

[92] *Cyber 101—Defend Forward and Persistent Engagement*, U.S. CYBER COMMAND (Oct. 25, 2022), https://www.cybercom.mil/Media/News/Article/3198878/cyber-101-defend-forward-and-persistent-engagement/.

[93] Dustin Carmack & Michael Ellis, *For Cybersecurity, the Best Defense Is a Good Offense*, HERITAGE FOUND., Nov. 10, 2021, https://www.heritage.org/technology/report/cybersecurity-the-best-defense-good-offense.

[94] Jim Garamone, *Esper Describes DOD's Increased Cyber Offensive Strategy*, U.S. DEPT. OF DEFENSE, https://www.defense.gov/News/News-Stories/Article/Article/1966758/esper-describes-dods-increased-cyber-offensive-strategy/.

[95] *Id.*

[96] Senator Ron Johnson, *Protecting Our Ability to Counter Hacking "PATCH" Act of 2017*, U.S. SENATE COMM. ON HOMELAND SEC. & GOVERNMENTAL AFF., https://www.hsgac.senate.gov/wp-content/uploads/imo/media/doc/PATCH%20Act_Background.pdf.

[97] Protecting Our Ability to Counter Hacking "PATCH" Act of 2017, H.R. 2481, 115th Cong. (2017).

[98] H.R. 2481, 115th Cong., § (2)(c)(1)(A) (2017).

[99] H.R. 2481, 115th Cong., § (2)(c)(1)(B)-(F) (2017).

Vol. 42, No. 1 (2023) ● ISSN: 2164-7984 (online) ● ISSN 0733-2491 (print)
DOI 10.5195/jlc.2023.270 ● http://jlc.law.pitt.edu

Security Council to participate at the request of the Board and with the approval of the President.[100]

The PATCH Act additionally pushes for more public disclosure of evaluation criteria as well as regular reports on VEP decision-making.[101] Section (f) of the PATCH Act[102] specifies that there must be annual reporting, including an unclassified version released to the public, to three committees in the Senate and four committees in the House of Representatives.[103]

The PATCH Act takes meaningful steps but does not do enough to effectively shift the decision-making process to ensure that previous failures of the VEP are not repeated. The PATCH Act takes good steps in pushing for more public disclosure of vulnerabilities, adding oversight mechanisms, and utilizing the DHS and NIST for evaluations and disseminations of vulnerabilities. However, overall decision-making and considered equities need to be changed to ensure that vulnerabilities are not stockpiled without a legitimate reason and that intelligence agencies are not falling into the same pitfalls that led to embarrassing leaks of valuable cyber weapons.

VI. PROPOSED REVISIONS/SOLUTIONS TO THE VEP

Regardless of whether the VEP undergoes significant change or remains the same, at a minimum, the current process should be codified into law. A codified process would ensure that there is not as much volatility in the decision-making process, the structure and process would be less subject to change, and that compliance with statutory requirements can be enforced.[104] This reflects sentiments in the VEP Charter, specifically in Section 5.2.4, where a goal of the VEP is to make determinations on vulnerabilities "based on repeatable techniques or methodologies" that enable an objective evaluation of risks and benefits.[105] Codification would allow for the process

[100] H.R. 2481, 115th Cong., § (2)(c) (2017).

[101] Mailyn Fidler & Trey Herr, *PATCH: Debating the Codification of the VEP*, LAWFARE BLOG (May 17, 2017), https://www.lawfareblog.com/patch-debating-codification-vep.

[102] H.R. 2481, 115th Cong., § (2)(f) (2017).

[103] Senate Committees: Committee on Homeland Security and Governmental Affairs, Committee on Commerce, Science, and Transportation, and the Select Committee on Intelligence; House Committees: Committee on Homeland Security, the Committee on Oversight and Government Reform, the Committee on Energy and Commerce, and the Permanent Select Committee on Intelligence.

[104] Lindsey Polley, To Disclose, or Not to Disclose, That is the Question xiii (2022) (executive summary) (Ph.D. dissertation, Pardee RAND Graduate School, RAND Corporation), RGSD-A1954-1.

[105] VEP Charter, *supra* note 12, at 7.

to be constant and have future decisions be made in a consistent and predictable way for all stakeholders involved. Additionally, the actual process to decide to restrict or patch would persist across administrations and would not be subject to the changes in policy preferences that happens with new leadership.

If Congress chooses to codify the VEP into law, they could also mandate the reporting of VEP decisions to Congress on a regular basis. While there are pros and cons to congressional oversight to specific issue areas, increasing public transparency into an area that rarely has insight would be a positive development. Reports to Congress would be retrospective, post-mortem type descriptions of how the VEP works in practice. As the PATCH Act states, there would be a public report that is disseminated widely; but, there could also be a classified version that is only shared with the House and Senate Select Committees on Intelligence. The original charter promised regular reporting and at the unclassified level, but no such reports have been released.[106]

A. Structural Changes to the VEP

The first changes that should take place are structural changes. Beginning with the leadership of the Equities Review Board, the ultimate decision-maker should be unbiased towards any of the interests represented by the members of the Board, whether permanent or ad hoc. The decision to disclose or restrict a vulnerability should be as unbiased as possible, and it should only be based on the criteria laid out by the process itself. These decisions should not be skewed towards the intelligence community (decision to restrict) or towards the private sector (decision to disclose). Ultimately, a strong, repeatable process based on objective criteria should be the guide in the decision-making process. After decisions are made, there should also be, at minimum, a short explanation for why the decision to disclose or restrict was made, citing specific equity considerations to ensure predictability and consistency. These statements need not be long judicial-style opinions but should clearly delineate which factors were most important in a given decision. This unbiased decision-maker could potentially be an official that is currently in the White House or National Security Council, or

[106] Senator Johnson, *supra* note 96.

a new position could be established and appointed with some kind of majority from members of the Equities Review Board.

B. Changes in Membership to the VEP

Next, there should be changes to the membership of the ERB to better represent private industry.[107] The PATCH Act proposes a dichotomy of permanent and ad hoc members of the ERB.[108] This is a good step, but it could go even further. In reflecting original purposes of the VEP from both the Charter and NSPD-54/HSPD-23, there should be a central focus on ensuring that the vulnerability is patched, and companies and individual citizens are protected. To better represent the private sector and certain industry groups, there could be an ad hoc industry representative involved in the VEP for vulnerabilities that impact a company in a certain industry. This ad hoc member could utilize existing frameworks of critical infrastructure set out by PPD-21.[109] For example, if a new vulnerability is found in a private company's software, there would be an industry representative for each sector of critical infrastructure[110] to represent the company's interests when decisions are made to restrict or disclose.

C. Changes to "Equity Considerations"

The next set of recommended changes regard the actual equity considerations that serve as decision-making factors on whether to disclose or restrict a vulnerability. The VEP Charter articulates a "primary focus" at the beginning of the document. That primary purpose is to enhance cybersecurity, protect core internet infrastructure, information systems, critical infrastructure, and the U.S. economy through disclosure of vulnerabilities.[111] The next phrase, however, suggests that those goals can only be overridden when there is a "demonstrable, overriding interest in the use of the vulnerability for lawful intelligence, law enforcement, or national

---

[107] Polley, *supra* note 104, at 101.
[108] H.R. 2481, 115th Cong., § (2)(c).
[109] PPD-21, *supra* note 1.
[110] Critical Infrastructure Sectors, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, https://www.cisa.gov/critical-infrastructure-sectors (last visited Sept. 14, 2023).
[111] VEP Charter, *supra* note 12, at 1.

security purposes."[112] This suggests that the default outcome of the VEP would be to disclose the vulnerability, not to restrict the vulnerability for the sole purpose of amassing a stockpile of cyberweapons. While it cannot be known with certainty what "demonstrable, overriding interest" means, that phrase seems to set a high bar for restricting a vulnerability.[113]

This default for disclosure should remain and should operate with additional restraint, so as to restrict vulnerabilities as a means of intelligence gathering only for narrowly tailored reasons. This type of scrutiny would limit restricting and using the vulnerability to the following very narrow circumstances: (1) when the use of the vulnerability is the only way to extract specific pieces of intelligence; or (2) when there are exigent circumstances.

Additionally, when the ERB decides to restrict a vulnerability the VEP process could also ensure that the vulnerability is eventually disclosed within a reasonable time period. This constraint should be put in place to ensure that the intelligence community is not stockpiling cyberweapons for hypothetical, future uses. Hopefully, with time constraints, situations such as the Shadow Brokers would not happen where a cache of powerful cyberweapons is stolen and released to the public.

These constraints would not necessarily mean that the intelligence community should stop hunting for zero-day vulnerabilities. Even if there are time and use constraints, disclosing vulnerabilities and seeing them through to patching is an overall net positive for the collective defense. Even if the NSA is limited to narrow use, or even a "one-shot" policy, they can still extract valuable intelligence. The original charter hints that there are different types of dissemination available to the ERB.[114] These dissemination options allow the intelligence community to sometimes continue using the vulnerability while the private sector works on patching. However, the overall outcome of any VEP decision should be disclosure within a reasonable time.

---

[112] *Id.*
[113] *See* Polley, *supra* note 104, at 102–03.
[114] VEP Charter, *supra* note 12, at 8.

Vol. 42, No. 1 (2023) ● ISSN: 2164-7984 (online) ● ISSN 0733-2491 (print)
DOI 10.5195/jlc.2023.270 ● http://jlc.law.pitt.edu

VII. OVERALL PROS AND CONS, ECONOMIC IMPLICATIONS OF A REVISED VEP

There are multiple trade-offs to a system such as the one proposed above. A revised process heavily skewed towards disclosure would result in safer software products that are widely used by companies and individuals. It would present private vendors with valuable support from their government for protecting critical systems and would enhance the public-private partnership in an area that has previously been the source of much distrust.[115] More disclosure could mean less data breaches, less impactful data breaches when they do happen, and a decrease in loss of money and sensitive information.

A policy of disclosure would also hopefully reduce the trade of zero-days on the DarkWeb. On the DarkWeb, there are entire criminal organizations and specific forums just for zero-day vulnerabilities.[116] The DarkWeb market operates largely in the shadows and involves mainly young hackers that do not have allegiance to any government and are motivated by money and an interest in showing off their skills to the highest bidder.[117] A policy of disclosure and further information sharing between the U.S. Government and major technology companies would help to reduce the activity of these DarkWeb forums, and reduce transnational cybercrime.

However, this approach also disincentivizes the private sector to take their own security more seriously. From one perspective, the NSA and the intelligence community are only one part of the greater "ecosystem" of cyberspace.[118] The vendor, at the end of the day, is responsible for the security of their own products and should shoulder the responsibility for the security of their own products. Additionally, there are legitimate companies that hunt and sell zero-day vulnerabilities to the intelligence community.[119] Default disclosure as a result of the VEP would significantly diminish the value of finding zero-days and, overall, diminish the value-add of these types of companies.

---

[115] Fidler & Herr, *supra* note 101.
[116] Fidler, *supra* note 2, at 415–16.
[117] PERLROTH, *supra* note 10, at 13–15, 17.
[118] Fidler & Herr, *supra* note 101.
[119] *Id.*

Vol. 42, No. 1 (2023) ● ISSN: 2164-7984 (online) ● ISSN 0733-2491 (print)
DOI 10.5195/jlc.2023.270 ● http://jlc.law.pitt.edu

Another issue is the significant extent to which the intelligence community has invested in the practice of finding and exploiting zero-days for intelligence purposes. In conjunction with their human intelligence partners at the CIA, the NSA has become prolific in breaking major software systems. For the NSA's Tailored Access Operations (TAO) division and its successor, the Computer Network Operations group, nothing is out of reach.[120] For example, in the early 2000s in the run-up to the Iraq and Afghanistan invasions, TAO was able to break into nearly anything, finding backdoors to nearly every major piece of technology.[121] This level of skill and intelligence collection has only grown. Suddenly, the NSA would be put in a difficult position where their ability to gain valuable intelligence would be severely hindered and significant resources spent on zero-day exploits would be essentially devalued.

VIII. CONCLUSION

In conclusion, the Vulnerabilities Equities Process is in need of reform. A history of aggressive intelligence gathering through private sector systems at the expense of the American taxpayer needs to be significantly changed. Refocusing the intelligence community to better partner with the private sector and to reduce cybercrime and large-scale hacks should be the goal of the VEP. With changes to structure, goals, and equities considered, the intelligence community can better secure the private sector of the United States while still being incredibly productive in their intelligence gathering mission. Using vulnerabilities in more limited scenarios is in the best interest of the intelligence community, the private sector, and everyday Americans. Ensuring consistency and public trust in the intelligence community is of paramount importance, and the proposed changes to the VEP will result in a better outcome for all stakeholders involved.

---

[120] *See* Ellen Nakashima, *NSA Employee Who Worked on Hacking Tools at Home Pleads Guilty to Spy Charge*, WASH. POST, Dec. 2, 2017, https://www.washingtonpost.com/world/national-security/nsa-employee-who-worked-on-hacking-tools-at-home-pleads-guilty-to-spy-charge/2017/12/01/ ec4d6738-d6d9-11e7-b62d-d9345ced896d_story.html.

[121] PERLROTH, *supra* note 10, at 108–11.

Vol. 42, No. 1 (2023) ● ISSN: 2164-7984 (online) ● ISSN 0733-2491 (print)
DOI 10.5195/jlc.2023.270 ● http://jlc.law.pitt.edu