REVAMPING THE VULNERABILITIES EQUITIES PROCESS

Sarah-Johanna Willcockson

INTRODUCTION

The evolution of zero-day vulnerability[1] detection and analysis is a technological progression and advancement in war

My sincere thanks to Andrew Carney, Technical SETA (contractor) in DARPA I2O, who helped inspire and edit this Note.

strategy and weaponry development. Relevant federal entities should adopt a legal framework to account for the shifting landscape in cyber vulnerability detection.

This article offers a brief history of the Vulnerabilities Equities Process (VEP) and proposes a legal regime for federal agencies' disclosure of zero-day vulnerabilities found in information systems and technologies. A VEP legal framework, created by subject-matter experts (SMEs) in the vulnerability reporting process, should account for the increased capacity of United States entities to find vulnerabilities, reduce opacity in the equity-weighing process, specify a default position toward coordinated disclosure, and be enforced through the weight and clarity of statutes.

I. VULNERABILITY DISCLOSURE AND THE VULNERABILITY EQUITIES PROCESS

Cyber vulnerabilities are defined as "weakness[es] in the computational logic (*e.g.*, code) found in software and hardware components that, when exploited, results in a negative impact to confidentiality, integrity, or availability."[2] Broadly speaking, the process of fixing—or "patching"—vulnerabilities involves "coding changes, but could also include specification changes or even

[1] "Zero-day vulnerability" is one that has been known to the vendor of the software with the vulnerability for 'zero-days' or, in other words, is a vulnerability that is not known to the owner of the vulnerable software. *See* Section I.E *infra* for discussion of zero-day vulnerability *Cf. See What is a Zero-day Exploit?*, KASPERSKY (2019) https://usa.kaspersky. com/resource-center/definitions/zero-day-exploit (last visited Mar. 31, 2021) (A "zero-day exploit" is "a cyber-attack that occurs on the same day a weakness is discovered in software… it's exploited before a fix becomes available from its creator.").

[2] *Vulnerabilities, National Vulnerability Database*, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, https://nvd.nist.gov /vuln, (last visited Mar. 31, 2021). The reference to "confidentiality, integrity, or availability" is a reference to the 'CIA triad,' which is a common metric for cyber security, generally. *See generally* Jeff Kosseff, *Hacking Cybersecurity Law*, 20 U. ILL. L. REV. 811, 831-34 (2020).

specification deprecations (*e.g.*, removal of affected protocols or functionality in their entirety)."[3]

Vulnerabilities reported to the National Vulnerability Database (NVD), maintained by the National Institute of Standards and Technology,[4] are given a Common Vulnerabilities and Exposures (CVE) identifier and are published to "the CVE" (list).[5] The CVE [list] is "a list of entries—each containing an identification number, a description, and at least one public reference—for publicly known cybersecurity vulnerabilities"[6] and may be used in commercial cybersecurity products.[7] The CVE is owned by the MITRE Corporation and sponsored by the Cybersecurity and Infrastructure Security Agency, part of the United States Department of Homeland Security (DHS).[8]

The United States Government (USG) and American public have an interest in maintaining the CVE and NVD since it allows commercial manufacturers to benefit from known reported vulnerabilities.[9] Thus, vendors of varying sizes and resources, including small businesses, benefit from the collective knowledge of a larger group.

Further, the creation of a publicly accepted and maintained list of vulnerabilities provides incentives for private hackers' participation in CVE reporting where hackers attain credibility by reporting previously unknown vulnerabilities to the CVE.[10] The ability

[3] *Vulnerabilities*, *supra* note 2.
[4] *General Information, National Vulnerability Database*, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, https://nvd.nist.gov/general, (last visited Mar. 31, 2021).
[5] *Vulnerabilities*, *supra* note 2.
[6] *CVE and NVD Relationship*, THE MITRE CORP., https://cve.mitre.org/about/cve_and_nvd_relationship.html (Dec. 11, 2020).
[7] *Id.*
[8] *Id.*
[9] *See generally id.*
[10] Social pressures to report vulnerabilities to the CVE are manifested in programs or metrics based on hackers' respective reporting capability *See e.g.*, *Reputation*, HACKERONE, https://docs.hackerone.com/ programs/signal-requirements.html (last

to track reported credible and relevant vulnerabilities in a professionally managed database translates, for hackers, into professional reputation and job opportunities and, for software vendors and USG agencies, a community of individuals willing to identify vulnerabilities capable of being exploited.[11] Consequently, maintaining a public database of known vulnerabilities encourages vulnerability disclosure among the private and government sectors. Disclosure of vulnerabilities also contributes to the public's ability to maintain high assurance cyber systems since disclosure protocols increase the amount of publicly available knowledge relating to software vulnerabilities, allowing vendors to patch software systems and contribute to software infrastructure security.

There is a substantial amount of literature relating to vulnerability markets (white, black, and otherwise), bug bounty programs,[12] and reasons for individual hackers to report, sell, or hoard their discovered vulnerabilities.[13] Efforts have been made to define and enforce "responsible vulnerability disclosure" at the private and

visited Mar. 31, 2021) ("A hacker's reputation measures how likely their finding is to be immediately relevant and actionable.") Signal is the average reputation hackers receive per report. The higher a hacker's signal is, the more reputable their report will be. *Signal and Impact*, HACKERONE, https://docs.hackerone.com/hackers/signal-and-impact.html (last visited Mar. 31, 2021) ("The higher a hacker's signal is, the higher the likelihood a submitted report will be reputable.")

[11] Jay P. Kesan & Carol M. Hayes, *Bugs in the Market: Creating a Legitimate, Transparent, and Vendor-Focused Market for Software Vulnerabilities*, 58 Ariz. L. Rev. 753, 759, 761, 820 (2016) ("[E]xploits are weaponized vulnerabilities").

[12] Bug Bounty programs allow cybersecurity researchers to report bugs to an organization and receive a form of compensation. *See generally* Ido Kilovaty, *Freedom to Hack*, 80 OHIO ST. L.J. 455, 484 (2019) ("At the same time, there are white-hat vulnerability markets, which are often referred to as 'bug bounty' programs, facilitated by the vendors themselves. These markets create incentives for security researchers by offering monetary rewards for reports of vulnerabilities made directly to the vendors under predetermined conditions. Their purpose is to create a greater incentive for security researchers to cooperate with vendors in order to prevent vulnerabilities from being sold to potentially malicious actors--criminal hackers and hostile governments.").

[13] *See e.g.*, *id.*; *see also* Taiwo A. Oriola, *Bugs for Sale: Legal and Ethical Properties of the Market in Software Vulnerabilities*, 18 J. MARSHALL COMPUTER & INFO. L. 451, 478 (2011).

academic levels.[14] This Note does not develop those issues, and focuses solely on vulnerabilities discovered by USG agencies and ensuing reporting procedures. The primary issues presented in this Note are whether a legal regime should govern USG agency's participation in protocols relating to disclosure of vulnerabilities, how transparent those protocols should be, whether the USG should consider disclosure to a publicly operated list (like the NVD), or to solely the affected vendor, and whether any legal framework should account for modern technological capabilities.

This Note addresses those issues by proposing the following: A codified VEP should be designed by SMEs in vulnerability discovery and reporting. It should account for the USG's improved ability to discover vulnerabilities. It should be more transparent than current VEP policies, particularly relating to metrics used to justify non-disclosure, and USG agencies should employ a vulnerabilities equities process that defaults to disclosure. The outcome of the process should be disclosure to affected vendors (coordinated disclosure). The outcome of the process should not be public disclosure, such as disclosure to a list like the NVD,[15] because the primary goal of the VEP

[14] *See generally Zero-day Initiative*, ZERO-DAY INITIATIVE, https://www.zerodayinitiative.com; *see also* ALLEN HOUSEHOLDER, GARRET WASSERMANN, ART MANION, CHRIS KING, THE CERT GUIDE TO COORDINATED VULNERABILITY. DISCLOSURE, (2017).

[15] For an example of an industry partner's found zero-day vulnerabilities being reported to the NVD after being identified as both exploitable and being used as exploits in-fact, *see* Maddie Stone, *In-the-Wild Series: October 2020 0-day Discovery*, Project Zero (Mar 18, 2021, 9:45 AM), https://googleprojectzero.blogspot.com/2021/03/in-wild-series-october-2020-0-day.html ("Project Zero closed out 2020 with lots of long days analyzing lots of 0-day exploit chains and seven 0-day exploits. When combined with their earlier 2020 operation, the actor used at least 11 0-days in less than a year."); *see also* Patrick Howell O'Neill, *Google's Top Security Teams Unilaterally Shut Down a Counterterrorism Operation*, MIT TECH. REV. (Mar. 26, 2021) https://www.technologyreview.com/ 2021/03/26/1021318/google-security-shut-down-counter-terrorist-us-ally/ (alleging the actors using the chain of exploits reported by Project Zero were "Western government operatives actively conducting a counterterrorism operation." While the article acknowledged the decision to use public disclosure is not a standard Google policy in response to such a situation, a former US intelligence official reportedly commented, "US allies don't all have the

should be highly defensible, secure software and hardware systems while minimizing disclosure of information with irreplaceable operational value.[16]

A. Government Disclosure

Where the USG is engaged in finding and exploiting vulnerabilities, there is arguably an "ethical imperative" to have a vulnerabilities equities process where the government weighs the risks associated with retaining a vulnerability for government-only usage against the risks of disclosing the vulnerability to the public or relevant software vendor.[17] The process necessitates a fact-bound inquiry since

ability to regenerate entire operations as quickly as some other players... The idea that someone like Google can destroy that much capability that quickly is slowly dawning on folks.").

[16] *See e.g.*, discussion of the Google's March 2021 full disclosure of the exploits allegedly being used in a Western counterterrorism operation, *supra* note 15; *see generally* Oliver Rochford, *Cyber War and the Compromise of Reliable Full Disclosure*, SECURITY WEEK, (May 14, 2008), https://www.securityweek.com/cyber-war-and-compromise-reliable-full-disclosure ("...we can't rely on our own governments to practice responsible full disclosure. Full Disclosure is compromised. We can't really blame them. Either everyone discloses, or no-one does. The game theory here is clear. But this competitive advantage comes at a steep price. Their own citizens and businesses are left exposed, reducing herd immunity for when the next agency is hacked, and the vulnerabilities are unceremoniously dumped on an unsuspecting internet."). *C.f.* Kevin Johnson, *Exposing the Fallacies of Security by Obscurity: Full Disclosure*, 5 ISACA J. 1, 1 (2017) ("Having another article talking about full disclosure and trying to convince you that it is a good idea may sound ridiculous, but bear with me.… While there are a number of arguments against full disclosure, such as that we cannot fix all of the problems disclosed or that patching is a difficult process in a modern, complex organization, it is still the right path to ensure comprehensive understanding of risk. And to be clear, I actually agree with both of those arguments against full disclosure. I just feel that they are outweighed by the benefits.")

[17] Stephanie Pell & LTC James Finocchiaro, *The Ethical Imperative for a Vulnerability Equities Process and How the Common Vulnerability Scoring System Can Aid that Process*, 49 CONN. L. REV. 1549, 1555-58 (2017); *see also* CYBER THREAT ALLIANCE AT THE CTR. FOR CYBERSECURITY POL'Y AND L., MORE SUNLIGHT, FEWER SHADOWS: GUIDELINES FOR ESTABLISHING & STRENGTHENING GOVERNMENT VULNERABILITY DISCLOSURE POLICIES (2021) ("It is crucial, therefore, that when government agencies come into possession of such vulnerabilities, that the government as a whole is able to weigh all relevant interests in determining whether

the associated risks of disclosure vary widely depending on numerous factors, including whether the vulnerability is exploitable, whether the relevant software system is widely used or part of critical infrastructure, and how likely the vulnerability will be found by a third-party.[18]

Where the USG weighs the offensive and defensive equities of a vulnerability disclosure, it generally considers the operational value of a vulnerability. A former member of the National Security Agency's (NSA) Office of Tailored Access Operations (TAO) (currently the Computer Network Operations) argues:

The business of offensive cyber operations, intelligence gathering, and hacking for law enforcement purposes increasingly requires the military, the intelligence community, and law enforcement to exploit networks, hardware, and software that are owned or produced by American companies. When USG agencies delay or fail to disclose zero-day vulnerabilities (presumably to exploit or continue exploiting such vulnerabilities), the information security of innocent Americans may be put at risk.[19]

To balance military, intelligence, and law enforcement interests against commercial and public interests in becoming situationally aware of vulnerabilities in its private and Department of Defense (DoD) software, the VEP was created.[20] The VEP an administrative process located in the executive branch that functions as a vetting tool for publishing USG found vulnerabilities to the public.[21]

---

to disclose those vulnerabilities to vendors immediately or to delay disclosure and use the retained vulnerabilities to advance specific operational goals. Doing so requires that governments have processes in place…") (available at: https://www.cyberthreatalliance.org/wp-content/uploads/2021/02/More_Sunlight_Fewer_Shadows-1.pdf).

[18] *Id.* at 1564.

[19] *Id.* at 1556-57.

[20] *Id.*

[21] CHRIS JAIKARAN, CONG. RESEARCH SERV., 7-5700, VULNERABILITIES EQUITIES PROCESS 1 (2017); *Common Vulnerabilities and Exposures (CVE)*, NATIONAL

The VEP has a narrow directive: to "evaluate the risks of delayed or non-disclosure of the vulnerability and weigh [it] against an agency's need to exploit the vulnerability."[22] While the machinations of the VEP remains an opaque procedure, some details about its structure, decision-making process, and purpose have been disclosed to the public.

A brief history is provided to contextualize the status quo VEP and its mandate.

B. Origin of the VEP

Created during the George W. Bush Administration, the National Security Presidential Directive (NSPD)—54 (also identified as Homeland Security Presidential Directive (HSPD)—23) provides that the Secretaries of State, Defense, Homeland Security, the Attorney General, and the Director of National Intelligence must create "a joint plan for the coordination and application of offensive capabilities to defend U.S. information systems."[23] Pursuant to this directive, these federal entities crafted the VEP to manage USG interests subsequent to a vulnerability discovery.[24] These actions were part of a larger USG-wide effort known as the Comprehensive National Cybersecurity Initiative, which called for cybersecurity education and supply chain risk analysis.[25]

INSTITUTE OF STANDARDS AND TECHNOLOGY, https://samate.nist.gov/BF/Enlightenment/CVE.html; *see also* Carlos Liguori, *Exploring Lawful Hacking as a Possible Answer to the "Going Dark" Debate*, 27 Mich. Tech. L. Rev. 317, 342 (2020).

[22] Pell & Finocchiaro, *supra* note 17, at 1558.

[23] Jaikaran, *supra* note 21, at 2 (quoting The White House, *HSPD-54/HSPD-23 Cybersecurity Policy*, Presidential Directive (2008), available at https://fas.org/irp/offdocs/nspd/nspd-54.pdf).

[24] *Id.*

[25] NATIONAL INSTITUTE OF STANDARD AND TECHNOLOGY, COMPREHENSIVE NATIONAL CYBERSECURITY INITIATIVE (Updated Sept. 26, 2017), https://csrc.nist.gov/Topics/Laws-and-Regulations/executive-documents/CNCI; *see also* Schwartz & Knake, *infra* note 27, at 4.

In 2014, a blog post written by then-Special Assistant to the President and Cybersecurity Coordinator, J. Michael Daniel, disclosed the VEP to the public.[26] The blog post stated there was a bias towards "responsibly disclosing [a] vulnerability" but stipulated there are "no hard and fast rules" governing the VEP's decision-making process.[27] It enumerated "considerations" the USG uses when weighing whether to disclose, including:

- "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?

[26] *Id.* The blogpost was part of the federal response to the Heartbleed vulnerability disclosure in which a vulnerability was found in the OpenSSL cryptographic software. Exploitation of the Heartbleed vulnerability could result in "disclosure of server private keys and sometimes sensitive credentials." INFOSEC INSTITUTE, HEARTBLEED OPENSSL 1.01A-1.01F (May 13, 2016), https://resources.infosecinstitute.com/lab-heartbleed-vulnerability/#gref. Both American and Canadian Government agencies reacted to the vulnerability disclosure by urging affected vendors to patch their systems. Jeffrey Roman, *Heartbleed: Gov. Agencies Respond,* BANK INFO SECURITY (Apr. 10, 2014), https://www.bankinfosecurity.com/heartbleed-government-agencies-respond-a-6737. The Obama Administration denied the National Security Agency (NSA) had advance knowledge of and exploited the Heartbleed vulnerability to gather intelligence, an allegation that was contradicted by a *Bloomberg* report which asserted the NSA had known about the Heartbleed vulnerability two years before it was publicly disclosed and the NSA had knowingly failed to protect Americans from the Heartbleed vulnerability. Mary Wheeler, *Why Obama's Response to the Heartbleed Bug is So Troubling*, THE WEEK (Apr. 14, 2014), https://theweek.com/articles/ 447844/why-obamas-response-heartbleed-bug-troubling. *See also* Michael Riley, *NSA Said to Have Used Heartbleed Bug, Exposing Consumers*, BLOOMBERG (Apr. 12, 2014, 12:00 AM), https://www.bloomberg.com/news/ articles/2014-04-11/nsa-said-to-have-used-heartbleed-bug-exposing-consumers. *See also* Michael Daniel, *Heartbleed: Understanding When We Disclose Cyber Vulnerabilities*, THE WHITE HOUSE (Apr. 28, 2014, 3:00 PM), https://obamawhitehouse .archives.gov/blog/2014/04/28/heartbleed-understanding-when-we-disclose-cyber-vulnerabilities.

[27] Daniel, *supra* note 26 at 1; *see also* ARI SCHWARTZ & ROB KNAKE, GOVERNMENT'S ROLE IN VULNERABILITY DISCLOSURE 2 (2016), available at https://www.belfercenter .org/sites/default/files/legacy/files/vulnerability-disclosure-web-final3.pdf.

- Does the vulnerability, if left unpatched, impose significant risk?
- How much harm could an adversary nation or criminal group do with knowledge of this vulnerability?
- How likely is it that we would know if someone else were exploiting it?
- How badly do we need the intelligence we think we can get from exploiting the vulnerability?
- Are there other ways we can get it?
- Could we utilize the vulnerability for a short period of time before we disclose it?
- How likely it is that someone else will discover the vulnerability?
- Can the vulnerability be patched or otherwise mitigated?"[28]

From the time of publication, critics pushed back on the opacity with which the VEP was run.

Notably, former Cyber Security Directors for the Cybersecurity Policy at the White House National Security Council, in a jointly published paper, argued the guidelines and criterion described in the Daniel blog post are employed at the discretion of current administration officials and should be codified if they are to remain relevant and transcend administrations.[29] They urged that, while a minority of VEP decisions must stay classified,

> [H]igh-level criteria that informs disclosure or retention decisions should be subject to public debate and scrutiny. Furthermore,

[28] Daniel, *supra* note 26, at 1.
[29] Schwartz & Knake, *supra* note 27, at 2.

> certain information about the implementation of the VEP, particularly the aggregate numbers of zero-day vulnerabilities discovered, the aggregate numbers of such vulnerabilities disclosed (as opposed to retained for government use), and the length of time that vulnerabilities are kept before disclosure, do not compromise sources and methods of how these vulnerabilities may have been discovered.[30]

Thus, they argue for "public and official release" of the information and warn against over-classification of VEP decisions.[31]

Despite an evolving library of public knowledge regarding the VEP that continues to be used by contemporary critics, these arguments remain relevant. Echoes of their reasoning were seen after a second disclosure of USG policy regarding the VEP.

C. The VEP Paper

In 2016, a disclosure of further information concerning the VEP occurred pursuant to a lawsuit between the Electronic Frontier Foundation and the NSA.[32] The partly redacted document, entitled "Commercial and Government Information Technology and Industrial Control Product or System Vulnerability Equities Policy and Process" ("VEP Paper"), gives a snapshot of the process the USG then used to weigh vulnerability disclosure (*see* Figure 1).[33] It was originally classified at the SECRET level and is dated February 16, 2010.[34] Explicitly stated within the VEP Paper and its "Highlights" attachment, the described equities balancing process was the end result of the plans created pursuant to the Bush Administration

[30] *Id.*
[31] *Id.*
[32] Elec. Frontier Found. v. NSA, No. 14-cv-03010-RS,2016 U.S. Dist. LEXIS 34870, at *2, *3 (N. D. Cal. Mar. 17, 2016).
[33] Schwartz & Knake, *supra* note 27, at 5-6; *Vulnerabilities Equities Process Highlights 7.8.2010*, ELECTRONIC FRONTIER FOUNDATION (2010), https://www.eff.org/document/vulnerabilities-equities-process-highlights-782010; *See also* Elec. Frontier Found, 2016 U.S. Dist. LEXIS 34870 at Exhibit B [hereinafter "VEP Paper Highlights"].
[34] VEP Paper, *supra* note 33, at 1.

NSPD-54 and provided for the "policy and responsibilities for disseminating information about vulnerabilities discovered by the [USG] or its contractors, or disclosed to the USG by the private sector or foreign allies in Government Off-The-Shelf (GOTS), Commercial-Off-The-Shelf (COTS), or other commercial information technology or industrial control products or systems (to include both hardware or software)."[35]

The VEP Paper states the articulated policy applies "to all components, civilian and military personnel, and contractors of the [USG] and to all hardware and software employed on government networks to include [GOTS], [COTS], or other commercial information technology or industrial control products or systems (to include open source software)."[36] Consequently, a literal reading of the application of the VEP policy indicates that application is widespread if not universal across the spectrum of DoD components. However, the ensuing policy is written in a way that makes reporting vulnerabilities to the VEP largely discretionary for most DoD entities.

Provision 5 of the VEP Paper provides that USG entities "shall introduce"[37] into the VEP any "vulnerabilities discovered by the USG or by non-USG entities under contracts with the USG, or disclosed to the USG by the private sector or foreign allies" that qualifies as

[35] VEP Paper, *supra* note 33, at 1; VEP Paper Highlights, *supra* note 33, at 1. For respective definitions of GOTS and COTS, *see* the VEP Paper, *supra* note 33, at 12.
[36] VEP Paper, *supra* note 33, at 1.
[37] Under the FAR § 2.101, which contains definitions of terms that govern the FAR and other DoD Regulations, including the DFARS and DGARS where terms are not defined within those documents, "must" and "shall" indicate an imperative. While DoD components are urged to use "must" instead of "shall" to indicate an imperative, the use of the word "shall" indicates an imperative and is used to impose a legal obligation on the reader. THE FEDERAL REGISTER DOCUMENT DRAFTING HANDBOOK, Office of the Federal Register (2017) (explaining the submission, format, and editorial requirements established in 44 U.S.C. § 15 (The Federal Register Act) and 1 C.F.R. § 1) ("Use of 'must' instead of 'shall' to impose a legal obligation on the reader"); THE FEDERAL PLAIN LANGUAGE GUIDELINES § (3)(a)(iv) (citing Federal Plain Writing Act of 2010, compels every federal department to "use 'must,' not 'shall' to indicate requirements."), https://www.archives.gov/federalregister/write /handbook.

Protected Critical Infrastructure Information (PCII).[38] If the vulnerability is not PCII, the USG entity that identifies the vulnerability is given the discretion to determine whether that vulnerability reaches the threshold for entry into the VEP.[39] The threshold for entering the VEP, given in Provision 6.4, is whether a vulnerability is "both newly discovered and not publicly known."[40] No other metrics are given.[41]

However, Annex C of the VEP Paper states a vulnerability is "publicly known" if:

> [T]he source of the information is a verbal or electronic presentation or discussion in a publicly accessible domain, or if there is a paper of other published documentation in the public domain… that specifically discusses the vulnerability under consideration and how the vulnerability could be exploited. This definition does NOT include information currently and properly protected as

[38] VEP Paper, *supra* note 33, at 2.
[39] *Id.* at 3 (VEP Provision 6.1(a)-(b)).
[40] *Id.* This metric confirms the assertion the VEP is focused on zero-day vulnerabilities. Pell & Finocchiaro, *supra* note 17, at 1563.
[41] VEP Paper, *supra* note 33, at 4.

Unclassified//For Official Use Only (U//FOUO)[42] or classified that has been inappropriately released to the public.[43]

Provision 6.2(d) of the VEP Paper stipulates that vulnerabilities discovered

> [D]uring the course of federally-sponsored open and unclassified research, whether in the public domain or at a Government agency… or other company doing work on behalf of the USG need not be put through the process. Information related to such vulnerabilities, however, does require notification to the Executive

[42] Unclassified//For Official Use Only. Information marked U//FOUO indicates a belief by the government that the information falls under an exemption to the Freedom of Information Act (FOIA) 2-9. FOUO is not a classification but is a protective marking. FOUO records "are unclassified official information which may be exempt from public release under one or more of the exemption categories of the FOIA. The fact that information is marked FOUO is not a basis for denying information requested under FOIA. The inverse is also true—the fact that information is not marked FOUO does not mean it can be released." Classification guidance generally stipulates that classification markings govern when both classified information and FOUO information are found on the same page. NATIONAL IMAGERY AND MAPPING AGENCY, GUIDE TO MARKING DOCUMENTS 41 (2001) (articulating guidance found in Executive Order (EO) 12958, "Classified National Security Information," and Director of Central Intelligence Directives (DCIDs)), https://fas.org/sgp/othergov/dod/nimaguide.pdf; *See also* DEPARTMENT OF DEFENSE MANUAL 5200.01, Volume 4 "DoD Information Security Program: Controlled Unclassified Information (CUI)" (As amended May 9, 2018), https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/ dodm/520001-V4p.PDF.

[43] *Id.* at 12. The last sentence in the definition likely means a vulnerability may be considered not "publicly known" where it is leaked in an unauthorized fashion and not subsequently acknowledged by a federal entity. *See e.g.* "EternalBlue" and "DoublePulsar," allegedly developed by the NSA, are exploits leaked to the public without authorization. Thus, if "EternalBlue" or "DoublePulsar" were exploits created by the NSA and had not been submitted to the VEP before being leaked, the NSA could likely not use the leak as an argument the exploits had become "publicly known" as a reason the exploits did not meet the threshold for submission to the VEP. *See generally* Scott Shane, *Malware Case is Major Blow for the N.S.A.*, The New York Times (May 16, 2007), https://www.nytimes.com/2017 /05/16/us/nsa-malware-case-shadow-brokers.html. This analysis, done in the hypothetical to illustrate an application of a principle, does not consider other reasons the NSA may be exempted from submitting the exploits to the VEP.

> Secretariat, which shall notify process participants for purposes of general USG awareness.[44]

A reading of Provisions 5, 6.4, and 6.2(d) together indicates that disclosure is only mandatory where the vulnerability pertains to PCII. Where the vulnerability does not qualify as PCII, the DoD component that discovered the vulnerability, given it is not a component devoted to federally-sponsored open and unclassified research or conducting such research, may use a two-prong test to decide whether disclosure of the vulnerability to the VEP is necessary. Under this two-prong test, the DoD component must decide whether the vulnerability is both newly discovered and not publicly known.

Per the Annex C definition of "publicly known," any vulnerability where the "*source* of the information" is in the public domain may be considered publicly known. This operant definition would allow for discerning DoD components to reason their way out of disclosing vulnerabilities with root information in the publicly accessible domain. Thus, Annex C's operant definition of "publicly known" significantly changes the discretion DoD components may exercise when considering whether a disclosure to the VEP is necessary. The definition and implications of "publicly known" are further discussed in Part I(F).

Next, the VEP paper illuminates portions of the VEP structure. The Executive Secretariat, a term first seen under provision 6.1, is required to notify VEP Points of Contact (POCs) of a reported vulnerability, and request VEP POCs respond if "they have an equity at stake and desire to participate in the decision process for that case."[45] Provision 6.5 provides the NSA/Information Assurance Directorate (which became the Capabilities Directorate, and is currently the New Cybersecurity Directorate and Capabilities) is the

[44] VEP Paper at 4. In practical application, this likely means that USG contracting agents and USG Agencies purposed for or conducting Research and Development (R&D) are not necessarily subject to VEP reporting requirements but may still be required to provide "information related to such vulnerabilities" to the Executive Secretariat.

[45] *Id.* at 3.

Executive Secretariat and its responsibilities are enumerated in Annex B of the VEP Paper.[46]

VEP POCs, as provided in provision 6.3, are the department/agency POC for each USG entity participating in the VEP, and are responsible for submitting vulnerabilities to the process and communicating with the Executive Secretariat.[47] Additionally, the VEP POCs are responsible for "ensuring that applicable cybersecurity, cyber defense, information assurance, intelligence, counterintelligence, law enforcement, or other offensive cyber operations equities of their organization are appropriately represented in the process."[48]

Once a VEP POC submits a vulnerability to the Executive Secretariat, the Executive Secretariat submits the vulnerability to the Equities Review Board (ERB), comprised of SMEs from participating USG entities.[49] The ERB is tasked with "render[ing] a decision for the USG on how to respond to the vulnerability."[50] If a participating USG entity disputes the decision of the ERB, the VEP Paper asserts there is an appellate process, but the appellate authority is redacted.[51]

Thus, under the VEP Paper, VEP POCs from participating agencies may submit vulnerabilities that meet the criterion of the two-prong test to the Executive Secretariat, located within the NSA Information Assurance Directorate. The Executive Secretariat submits the vulnerabilities to the VEP POCs from other agencies—if that agency has an equity at stake—and to the ERB. The ERB decides whether to retain or disclose the vulnerability. This decision may be appealed, but the appellate authority is redacted.[52]

[46] *Id.* at 5, 11.
[47] *Id.* at 5.
[48] *Id.*
[49] *Id.* at 3; the agency members of the ERB are not specified. *See* discussion of provision 7, *infra* Part I(C).
[50] VEP Paper, *supra* note 33, at 4.
[51] *Id.*
[52] *See* Figure 1 to this Note.

The equities that are to be weighed by the ERB are enumerated and defined in Annex A of the VEP Paper.[53] They are: defensive cyber operations community equities, offensive cyber operations community equities (definition redacted), law enforcement equities, counterintelligence equities (definition partially redacted), and "other equities."[54]

These weighed community equities stand in contrast to the "considerations" listed by the Daniel blog post, which revealed a more granular factorial system. The 2014 Daniel blog post, released after the VEP was created in 2010, likely gave insight into the analysis conducted within the weighing of community equities described by the VEP paper. For instance, the "considerations" given by the Daniel blog post (*e.g.*, "How likely is it that we would know if someone else were exploiting it? Could we use the vulnerability for a short period of time before we disclose it?") are questions that may be asked within each of the broad categories of the VEP Paper's equities (*e.g.*, "defensive cyber operations community equities," "offensive cyber operations community equities").

The contrast between the Daniel blog post and the VEP Paper reveal the delta between what the USG was comfortable releasing to the public voluntarily and information the administration let slip through its fingers only after a drawn-out lawsuit. While the release of the VEP Paper provided greater clarity on the governmental process used to determine whether to release vulnerabilities, and what communities were given equities to be considered, key pieces of information were still missing after the release of the VEP Paper.

First, while Provision 7 details a mechanism for oversight in the event a USG entity disputes the conclusions of the ERB, the

[53] VEP Paper, *supra* note 33, at 10.

[54] *Id.* According to the Annex A, "Other Equities," are relevant where "some USG entities may not have equities that fall under those mentioned but, while executing their roles/responsibilities, they will be affected by the vulnerability or they have responsibilities that should be considered as part of the decision process (*e.g.*, Department of State, Department of Energy, Department of Commerce, *et al*)."

overseeing entity is redacted.[55] Consequently, it is unclear on what grounds an ERB decision may be appealed or whether the overseeing entity is a suitably "neutral and detached"[56] magistrate or subject to adequate oversight.[57] The identity of the appellate authority is particularly important given the public's lack of data on how well the VEP is working, or whether the oversight process is adequate.

Second, also per Provision 7, it is unclear how the public may measure the effectiveness of the VEP. Under this Provision, the Executive Secretariat collects annual reports from unspecified "departments and agencies" on the status of the reported vulnerabilities and the effectiveness, timeliness, and relevancy of the VEP.[58] Those reports are not released to the public or necessarily sent to Congress, the American public's appointed representatives. The lack of public information regarding the performance evaluations of the VEP and the opaque oversight mechanism is problematic. Awareness of how well the VEP is operating is crucial to public understanding of whether the USG is responsibly weighing risks associated with vulnerability disclosure. Further, lack of stipulated Congressional oversight removes a check on the executive's process of weighing offensive and defensive equities where the executive branch's dog in the fight is the "competitive enterprise of ferreting out crime"[59] or, in some cases, national security risks.[60] Because the decision to disclose or retain a vulnerability relates to the ability of the

[55] *Id.* at 8-9.
[56] *Johnson v. Unites States*, 333 U.S. 10, 14 (1948).
[57] VEP Paper, *supra* note 33, at 8-9.
[58] *Id.*
[59] *Johnson*, 333 U.S. at 14.
[60] *See generally* Ahmed Ghappour, *Searching Places Unknown: Law Enforcement Jurisdiction on the Dark Web*, 69 STAN. L. REV. 1075, 1132-36 (2017) (Arguing the best oversight for USG "network investigative techniques" is Congressional oversight since the judiciary is constrained by jurisdictional issues, a deference to law enforcement, and much of cyber policy remains under the domain of the executive branch since it falls within the powers of crafting foreign policy and national security strategy. Where Congress is adequately informed of VEP proceedings it may "indirectly control law enforcement's procurement of malware tools through line item adjustments or by barring the use of funds to procure tools that do not comply with the vulnerability equities process.")

government to investigate crime or otherwise use a vulnerability operationally, the process should include oversight by either the judiciary or Congress, because these branches have historically served as a check on the executive branch's use of law enforcement, investigative, intelligence tools, or military endeavors.[61]

Third, the VEP Paper never enumerates the VEP's participating USG entities.[62] Without knowing which federal entities are weighing interests, the public cannot infer if there is a balanced representation of interests or if all interests are represented. For instance, if the ERB consists of primarily Intelligence Community representatives and relatively few entities representing commercial or consumer interests, the weighing of equities may favor retention of a vulnerability for operational value regardless of whether there is a stated policy in favor of disclosure. The potential lack of consumer interests represented in the ERB is particularly notable because it is potentially consumer data at risk where the government keeps a vulnerability undisclosed for ongoing operational value.

Next, the VEP Paper lacks legal enforcement provisions.[63] There are no stipulated penalties for a USG entity failing to disclose a vulnerability that meets the threshold requirements, and no references to an Executive Order (EO) or statute providing the force and effect of law.[64] Critics have argued the USG has "confused a public relations

[61] *See generally* Shima Baughman, *Subconstitutional Checks*, 92 NOTRE DAME L. REV. 1071, 1071 (2017) (reasoning that "legislatures limit actions of police and prosecutors; and courts enforce individual constitutional rights and stop executive misconduct." [*sic*]); *See also* John Yoo, *The Continuation of Politics by Other Means: The Original Understanding of War Powers*, 84 CALIF. L. REV. 167, 190-91 ("'original constitutional materials indicate that the Framers intended a narrowly circumscribed presidential war-making power, with the Commander in Chief Clause conferring minimal policy-making authority' except in the case of sudden attacks… 'the President's designation as Commander in Chief, then, appears to have implied no substantive authority to use the armed forces, whether for war (unless the United States were suddenly attacked) or for peacetime purposes, except as Congress directed.'") (quoting Michael J. Glennon, Constitutional Diplomacy (1990)).
[62] VEP Paper, *supra* note 33, at 3.
[63] *Id.*; *See generally* Pell & Finocchiaro, *supra* note 17, at 1563.
[64] *See generally* VEP Paper, *supra* note 33.

strategy with a security strategy" and the VEP does little more than provide political cover for the USG when caught in a vulnerability-related scandal.[65]

The VEP Paper paints a picture of a policy that applies to all of DoD, including contractors, but is enforceable against no one. Apart from the requirement vulnerabilities related to PCII be disclosed, the threshold for submission to the VEP is vague and easily pliable.[66] If a vulnerability is submitted to the VEP, the equities used to weigh whether to disclose the vulnerability "external to the USG" are skeletal and, in several instances, redacted definitions of DoD communities. Further, there is no explicit consideration of consumer or vendor interests apart from the possibility that those interests may be subsumed under "other equities." These interests are paramount to the weighing process because it is often the exposed vendor, whose software contains the vulnerability, that is assuming the risk of the vulnerability being exploited by a third-party hacker. The VEP Paper stands for the proposition that a vulnerabilities equities process exists, but without stated representation from the potential victims of the discovered vulnerabilities, the force and effect of law, or an identifiable oversight mechanism.

However, public knowledge of the VEP has continued to evolve, and the VEP Charter has replaced the VEP Paper.

D. The VEP Charter

In November 2017, the former cybersecurity coordinator for the Trump Administration, Rob Joyce, published an unclassified

[65] Dave Aitel & Matt Tai, *Everything You Know about the Vulnerability Equities Process Is Wrong*, LAWFARE (Aug. 18, 2016, 2:46 PM), https://www.lawfareblog.com/everything-you-know-about-vulnerability-equities-process-wrong.

[66] The stipulation that a vulnerability may be "publicly known" if the *source* of the information relating to the vulnerability is publicly known, in particular, provides leeway to agencies seeking to avoid disclosure by claiming that the software in which the vulnerability is found is publicly available *e.g.*, COTS Software. VEP Paper at 12.

version of the VEP Charter.[67] It describes the participating agencies and the regulatory regime governing the process.[68] The VEP Charter provides that it supersedes the VEP Paper but does not supersede any other existing law, policy, or regulation.[69] It does not codify the VEP or otherwise cause VEP policy to have the force and effect of law.[70]

Congruent with preceding VEP documents, the VEP Charter reveals a process intended to default to disclosure "absent a demonstrable, overriding interest in the use of the vulnerabilities."[71] Despite some similarities, differences between the documents indicate either changes in VEP policy or that an additional piece of VEP policy has been thrown into relief (*see* Figure 2).

First, the VEP Charter states the object of the vulnerability disclosure is necessarily to the "vendor/supplier" while the VEP Paper more ambiguously draws a binary line between keeping a discovered vulnerability internal or "external to the USG."[72] Thus, under the VEP Charter, the USG weighs whether to disclose solely to the vendor/supplier ("coordinated disclosure") while, under the VEP Paper, the USG theoretically weighs equities for disclosure to a variety of interested parties, including the public at large ("full disclosure").[73] This nuanced shift in purpose is consistent with the apparent consensus among industry and governmental entities that the primary

[67] Sven Herpig & Ari Schwartz, *The Future of Vulnerabilities Equities Processes around the World*, LAWFARE (Jan. 4, 2019, 12:30 PM), https://www.lawfareblog.com/future-vulnerabilities-equities-processes-around-world; "Vulnerabilities Equities Policy and Process for the United States Government" (Nov. 15, 2017) available at https://trumpwhitehouse.archives.gov/sites/whitehouse.gov/files/images/external%20-%20Unclassified%20VEP%20Charter%20FINAL.PDF [hereinafter VEP Charter].
[68] VEP Charter at 1-2.
[69] VEP Charter at 2.
[70] VEP Charter.
[71] VEP Charter at 1.
[72] VEP Charter at 1; VEP Paper at 2.
[73] The decision to disclose a vulnerability solely to the vendor/supplier is referred to as "coordinated disclosure" as opposed to "full disclosure" which is the decision to inform the public without necessarily coordinating with the vendor/supplier. Ablon & Bogart, i*nfra* note 100, at footnote 13.

rationale for governmental disclosure is to facilitate vendors in patching vulnerabilities.[74]

Second, the VEP Charter enumerates a non-exhaustive list of agencies and departments that comprise the ERB.[75] It states a "VEP Director at the [National Security Council]" will "be responsible for ensuring effective implementation of VEP policies" and "the VEP Director is the Special Assistant to the President and Cybersecurity Coordinator."[76] The structure of the VEP is further clarified by the revelation that the Executive Secretariat, still part of the NSA, acts directly under the direction of the Secretary of Defense (SECDEF) when executing VEP responsibilities.[77]

Third, the VEP Charter specifies an annual VEP report be written at the lowest classification level possible and should include an executive, unclassified summary that "*may* be provided to the Congress."[78]

Moreover, while the VEP Charter, on its face, keeps the VEP Paper's threshold for submitting vulnerabilities— "newly discovered and not publicly known"—it changes the definitions of the terms in Annex A.

E. VEP Paper and VEP Charter Compared: "Newly Discovered"

In contrast with the VEP Paper, which does not define "newly discovered,"[79] the VEP Charter asserts a "newly discovered" vulnerability is a zero-day vulnerability the USG discovers or new

[74] Susan Hennessey, *Vulnerabilities Equities Reform that Makes Everyone (And No One) Happy*, LAWFARE (July 8, 2016, 12: 27 PM), https://www.lawfareblog.com/vulnerabilities-equities-reform-makes-everyone-and-no-one-happy ("But all critics—and indeed the US government—appear to agree that the reason to disclose a vulnerability is to patch it and eliminate the threat.").
[75] VEP Charter at 3-4.
[76] VEP Charter at 4.
[77] VEP Charter at 4.
[78] VEP Charter at 5 (Emphasis added.) (Discussed infra in Part II(C)).
[79] *See* VEP Paper at 5, 12-13.

zero-day vulnerability information the USG discovers.[80] Neither this definition nor the definition of USG in paragraph 1 of the VEP Charter indicates whether agents of the USG, *e.g.*, contractors, may be included in this definition. This represents a change from the provisions in the VEP Paper which specified the policy applied "to all civilian and military personnel, and contractors of the [USG]."[81] Even more than the lack of specification present in the VEP Charter, the active change in language may indicate a slight alteration in position. In other words, the added definition of "newly discovered" may be interpreted to solely apply to those vulnerabilities discovered by federal employees. If true, this would be a shift in policy.

Additionally, within Annex A, the VEP Charter operantly defines a zero-day vulnerability as having three conjunctively connected preconditions. According to the Annex, a zero-day vulnerability must be: (1) unknown to the vendor; (2) exploitable; and (3) not publicly known. Annex A provides that a "publicly known" vulnerability is one where the "vendor is aware of its existence and/or vulnerability information can be found in the public domain."[82]

The Annex A definition of "zero-day vulnerability" means that vulnerabilities thought not to be exploitable are not subject to the VEP threshold.[83] This intuitively makes sense because it allows for the VEP to focus its temporal and otherwise finite resources on vulnerabilities with actionable exploits. The requirements that the vulnerability be "unknown to the vendor" and "not publicly known," defined as unknown to the vendor and/or present in the public domain, means that a found vulnerability that is known to the vendor but not in the public domain does not meet the VEP threshold. This distinction is congruent with the VEP Charter's stated purpose of weighing equities to determine whether to report the vulnerability to

[80] VEP Charter at 11-12.
[81] VEP Paper, *supra* note 33, at 1.
[82] VEP Charter at 12.
[83] It is acknowledged that a vulnerability that is not initially exploitable may become exploitable in the future, but, given the VEP has limited time and resources, it is likely not feasible to require it to vet vulnerabilities based on hypothetical risk. *See generally* Ablon & Bogart, *infra* note 100, at 17.

the vendor—not the public or other interested parties. Under the VEP Charter, the litmus test is the state of mind and interests of the vendor—not value added to public discussion or the public's situational awareness—an issue addressed, and a benefit sought after by other systems, such as the maintenance of the CVE.

F. VEP Paper and VEP Charter Compared: "Publicly Known"

In contrast to the VEP Paper, the VEP Charter's definition of "publicly known" does not carve out the specification that "publicly known" vulnerabilities exclude those marked U//FOUO, or classified vulnerabilities that have been inappropriately released to the public.[84] Thus, the VEP Charter's definition of "publicly known" may include those vulnerabilities known to the vendor and within the public domain, even if the origin of the information was an unauthorized leak.[85] This alternation may remove any pressure for needless analysis over whether a leaked vulnerability—a vulnerability that is consequently functionally public—be disclosed.

A further distinction between the VEP Paper's definition of "publicly known" and the VEP Charter's definition of "publicly known" is the VEP Charter's simplification of the analysis to determine what is "publicly known," and a broadening of the scope of vulnerabilities that may be considered "publicly known."

Under the VEP Paper, a vulnerability was not publicly known if "the source of the information is… in a publicly accessible domain, or if there is a [published document] in the public domain that specifically discusses the vulnerability and how that vulnerability could be exploited."[86] This definition allowed vulnerabilities to be excluded from the VEP if the source of the information was in the public domain—not necessarily the vulnerability itself. Additionally, the conjunctive structure of the second clause indicates that if the vulnerability was published in the public domain, but the knowledge

[84] VEP Charter at 12; VEP Paper, *supra* note 33, at 12.
[85] *Id.*
[86] VEP Paper at 12.

of how the vulnerability may be exploited was not published to the public, the vulnerability may not be considered publicly known for the purpose of whether it meets the VEP threshold. Thus, USG entities could withhold vulnerabilities from the VEP if it could be argued the *source* of the vulnerability information is publicly known, or the *mechanism for exploitation* is unknown to the public.

These two safe harbors are erased by VEP Charter language, which states a vulnerability is not publicly known if the "vendor is aware" of its existence and "its existence and/or vulnerability information can be found in the public domain." There is no distinction between vulnerability source information and vulnerability information. Also, there is no specification that the mechanism for exploitation be known to the public. Consequently, the VEP Charter's definition may require more vulnerabilities be reported to the VEP. Again, the rationale for this broadening may be that the VEP's narrowed purpose under the VEP Charter is whether to inform the vendor of the vulnerability and is not purposed to weigh the decision to inform the public. There is potentially less operational value lost from a coordinated disclosure than from a full disclosure so, under the coordinated disclosure regime of the VEP Charter, it may be more equitable to increase vulnerability reporting to the VEP so more vulnerabilities are considered against the lesser cost of coordinated disclosure.

G. VEP Paper and VEP Charter Compared: Equities Considered

The considered equities in the VEP Paper are listed under Annex A of the VEP Paper and the considered equities in the VEP Charter are listed under Annex B of the VEP Charter.

As previously discussed, the equities in Annex A of the VEP Paper are the definitions of offensive and defensive cyber operations community equities, law enforcement equities, counterintelligence equities, and "other equities." There are no factors to be weighed within those broad categories and no indication of a value encoding

system to indicate if some categories are weighed more heavily than others.

The VEP Charter diverges from the VEP Paper's indefinite approach and gives a detailed list of considerations, including sub-factors to be weighed within the broad categories of defensive, intelligence, law enforcement, operational, commercial, and international partnership equity considerations. Notably, the latter two categories are novel to the VEP Charter and indicate a broadening of considered equities beyond the interests associated with USG agencies and departments. The VEP Charter, in Provision 2, also explicitly acknowledges the wider array of interests beyond national security when it states, "[v]ulnerabilities can have significant economic, privacy, and national security implications when exploited."

Detailed academic reporting has been done on the value of weighing these respective equities and the tension between operational and public interests.[87] Critics of the VEP argue the VEP is an example of restrictions and scrutiny applied to USG cyber operations that are not reciprocally applied to USG adversaries.[88] It is also asserted that a VEP untethered from technical and objective metrics hampers the USG's ability to solve the "going dark" issue.[89] These arguments, meritorious or not, are beyond the scope of this Note. Instead, the following analysis concerns how the VEP, conceived of and constructed before the rise of the smartphone or USCYBERCOM became operational,[90] requires updated legal

[87] *See generally*, Vanessa Sauter, *Vulnerabilities Equities Process Charter*, LAWFARE (Nov. 15, 2017, 10:48 AM), https://www.lawfareblog.com/document-vulnerabilities-equities-process-charter; *See also* Aitel & Tai, *supra* note 65.
[88] *See* Aitel & Tai, *supra* note 65.
[89] *Id.*; *See also* Jonathan Mayer, *Government Hacking* 127 YALE L. J. 570, 570-73 (2018) (reasoning that, as the private sector becomes more sophisticated at using encryption and anonymization tools, the government must increasingly "resort to malware" to accomplish law enforcement and national security objectives) available at https://www.yalelawjournal.org/pdf/Mayer_k3iy4nv8.pdf.
[90] *U.S. Cyber Command History*, U.S. CYBER COMMAND, https://www.cybercom.mil/About/History/ (USCYBERCOMMAND reached Initial Operational Capability on May 21, 2010).

regulation to account for status quo public interests and governmental abilities.

II. SUGGESTED CHANGES

A. Status Quo

The progression from the VEP Paper to the VEP Charter has resulted in a vulnerability reporting structure that, despite calls for transparency and codification dating back to the initial VEP blog post, is still opaque and nominal.[91]

Efforts to codify the VEP have thus far failed. Attempts include the following: Protecting our Ability to Counter Hacking (PATCH) Act (2017) (House Resolution 2481 and Senate Bill 1157, respectively, introduced in both the House and Senate and did not progress from committee), House Resolution 6237, "Matthew Young Pollard Intelligence Authorization Act for Fiscal Years 2018 and 2019" (passed the House and did not progress), Senate Bill 3153, "Matthew Young Pollard Intelligence Authorization Act for Fiscal Years 2018 and 2019" (introduced into the Senate and did not progress), and House Resolution 3202, "Cyber Vulnerability Disclosure Reporting Act" (passed the House but did not progress).

Recently, as of September 2, 2020, the Department of Homeland Security (DHS) issued a Binding Operational Directive (BOD) stipulating that USG agencies implement a Vulnerability Disclosure Policy (VDP) for vulnerability reporters who find vulnerabilities in agency systems.[92] The DHS BOD is reportedly a reaction to the "lack of Federal progress" on codifying vulnerability disclosure protocols in an era with increasing cybersecurity problems and reports of vulnerability disclosure policy not being consistently implemented across DoD.[93] The DHS BOD actualizes a vulnerability disclosure process different from the VEP contemplated by the VEP

[91] Daniel, *supra* note 26, at 1.
[92] Department of Homeland Security, Binding Operational Directive 20-01 (Sept. 2, 2020) available at https://cyber.dhs.gov/bod/20-01/.
[93] *Id.*

Paper and VEP Charter in that it legally requires, per 44 U.S.C. § 3553(b)(2), each USG agency create a VDP for vulnerabilities found in agency software discovered by private actors, rather than mandate each agency participate in a DoD-wide VEP for consideration of vulnerabilities found by USG personnel.[94] Consequently, while it is a step forward in codifying vulnerability reporting where the vulnerability is found in agency software by private actors, it is a protocol separate from the VEP contemplated by the VEP Paper and VEP Charter.

Given neither the VEP Paper nor the VEP Charter have the force and effect of law, a legal framework does not regulate USG full or coordinated disclosure. This is likely because technological restrictions and voluntary policy practices have thus far created an acceptable homeostasis where harm is not overburdening technological industry partners, the USG, or the public, to the point that any group has adequately demanded legal action.

It does not necessarily follow that VEP procedures have secured public trust or proven optimally effective. For instance, WannaCry ransomware, deployed on May 12, 2017, across multiple countries—approximately 7 months before the public release of the VEP Charter—was arguably crafted using the "EternalBlue" and "DoublePulsar" exploits the NSA allegedly created. [95] Only after the exploit became likely to be used to effectuate harm did the NSA assist Microsoft, the targeted vendor.[96] Microsoft has joined numerous other

[94] *Id.*

[95] Maxat Akbanov et al., *WannaCry Ransomware: Analysis of Infection, Persistence, Recovery Prevention and Propagation Mechanisms*, J. OF TELECOMM. & INFO. TECH. 113, 114 (2019); *See also* Shane, *supra* note 43.

[96] Lily Newman, *The Leaked NSA Spy Tool that Hacked the World*, Wired (March 7, 2018, 8:00 AM), https://www.wired.com/story/eternalblue-leaked-nsa-spy-tool-hacked-world/ ("In the aftermath of WannaCry, Microsoft and others criticized the NSA for keeping the EternalBlue vulnerability a secret for years instead of proactively disclosing it for patching."); *Shadowbrokers*, DARKNET DIARIES Ep. 53 (Dec. 10, 2019) (downloaded using Podbean and Google Play) (Interview with Jake Williams from Rendition Security and former NSA TAO member. EternalBlue was leaked by a group known as "Shadowbrokers." The group's preceding leaks may have caused reasonable persons to believe that leaks such as EternalBlue were

technological giants in criticizing the NSA for keeping, specifically, the EternalBlue vulnerability secret instead of disclosing it for the purpose of patching.[97] EternalBlue is still weaponized against governmental and commercial platforms and has allegedly been used by both private and nation-state actors, including, allegedly, the Russian group known as Fancy Bear, to hack into USG software systems.[98] The alleged ability of the NSA to "hoard" the zero-day exploits used to create WannaCry may be perceived as a canary in the coal mine, indicating the VEP is not adequately serving vendor or public interests.[99]

On the other hand, there is an empirically demonstrated operational interest in concealing USG discovered vulnerabilities to weaponize them against USG adversaries. To illustrate, Stuxnet, a high-profile cyber operation effectuated against Iran, and widely believed to be a product of NSA engineering, relied on four Microsoft zero-day vulnerabilities to create an exploit that could simultaneously deaccelerate and accelerate centrifuges while causing the nuclear reactor monitoring software to report routine operation.[100] Additionally, while not publicly confirmed, many suspect the

imminent and, thus, the NSA took action in the form of a coordinated disclosure. However, this coordinated disclosure may be seen as "too little too late" since widespread application of the patch was not possible in the time between NSA's coordinated disclosure and when the Shadowbrokers effectuated the EternalBlue leak).

[97] *Id.*

[98] *Id.*

[99] *See* Kesan & Hayes, *supra* note 11, at 753, 793 ("The Shadow Brokers dump strengthens our conviction that the hoarding of zero-days by any government runs counter to public interest." [*sic*]); *See also* Lily Newman, *WikiLeaks Just Dumped a Mega-Trove of CIA Hacking Secrets*, WIRED (March 7, 2017, 11:40 AM) https://www.wired.com /2017/03/wikileaks-cia-hacks-dump/ (arguing CIA leaks reveal the CIA was hoarding exploits relevant to many common operating systems that put the public at risk, including unpatched iOS, Windows, and Android vulnerabilities.).

[100] Lillian Ablon & Andy Bogart, *Zero-days, Thousands of Nights*, RAND CORP. RES. REP. 1, 3 (2017) available at https://www.rand.org/pubs/research_reports/RR1751.html.

Heartbleed vulnerability[101] was operationalized before it became publicly known.[102]

The Heartbleed vulnerability may serve as a microcosmic example of the delicate balance between accommodating operational interests and protecting citizens relying on American software security. The Heartbleed vulnerability allegedly served an operational function that furthered intelligence operations[103] but was eventually weaponized against an unsuspecting public due to the alleged USG decision to retain the zero-day vulnerability until it was exploited by a third-party.[104]

The Heartbleed vulnerability may also stand for the proposition that the status quo is allowing for the hoarding of critical vulnerabilities without an *apparent* trade-off in operational value (this necessitates a level of speculation since operational value, by its nature, is not necessarily fully knowable in an unclassified space), causing a potential degradation of public trust. While the harm created by the Heartbleed exploit is well known, the value-added while it was retained for government usage is, at best, a subject of speculation.[105] A function of classifying victories and bearing public failures, an issue generalizable across many components in the DoD, is a trade on public trust that, even if the public cannot see behind the curtain, they trust that those running the show are acting in their best interest.

This trust is valuable and should not be exploited unnecessarily, particularly if trust levels are running low. Roughly 49% of Americans do not feel "confident" their government is capable of protecting data,[106] roughly 67% of US consumers think the USG

[101] *See* Riley, *supra* note 26.
[102] Ablon & Bogart, *supra* note 100.
[103] *Id.*
[104] Riley, *supra* note 26.
[105] *Id.*
[106] A.W. Geiger, *How Americans Have Viewed Government Surveillance and Privacy Since Snowden Leaks*, PEW RSCH. CTR. (June 4, 2018), https://www.pewresearch.org/fact-tank/2018/06/04/how-americans-have-viewed-government-surveillance-and-privacy-since-snowden-leaks/ (quoted in Mimana

should be more actively protecting data privacy,[107] and a historically low percentage of Americans—approximately 17%-- trust the government to "do what is right."[108] Moreover, wariness of unlawful government surveillance remains a present issue, as demonstrated by public reaction to Coronavirus contact-tracing applications on phones, the specter of government issued applications to track and monitor Coronavirus outbreaks, or the muted but wary public reaction to the report that DHS authorized its employees to collect information on protesters perceived to be threatening monuments in the Summer of 2020.[109] Thus, as argued since the VEP became public,

---

Ambastha, *Taking a Hard Look at the Vulnerabilities Equites Process and its National Security Implications*, BERKLEY TECH L.J. BLOG (Apr. 22, 2019), http://btlj.org/2019/04/taking-a-hard-look-at-the-vulnerable-equities-process-in-national-security/#_ftnref22).

[107] *SAS Survey: 67 Percent of US Consumers Think Government Should Do More to Protect Data Privacy*, SAS (Dec. 10, 2018), https://www.prnewswire.com/news-releases/sas-survey-67-percent-of-us-consumers-think-government-should-do-more-to-protect-data-privacy-300761765.html (N = 525, the demographic was American "adult consumers;" the full report is available in an e-book here: https://www.sas.com/en/whitepapers/data-privacy-110027.html); *see also* Brooke Auxier & Lee Rainie, *Key takeaways on Americans' Views about Privacy, Surveillance and Data-Sharing*, PEW RSCH. CTR. (Nov. 15, 2019), https://www.pewresearch.org/fact-tank/2019/11/15/key-takeaways-on-americans-views-about-privacy-surveillance-and-data-sharing/ (stating the majority of Americans feel concerned at how much the government (64%) and private sector (79%) is collecting about them, feel their information is less secure than it was five years ago (70%), and the majority (84%) feel very little or no control over the data collected about themselves by the government where N= 4,272 U.S. adults between June 3 and 17, 2019 with an overall margin of error plus or minus 1.87 percentage point).

[108] *Public Trust in Government: 1958-2019*, PEW RSCH. CTR. (Apr. 11, 2019), https://www.people-press.org/2019/04/11/public-trust-in-government-1958-2019/.

[109] *See* Derek Thompson, *The Technology That Could Free America From Quarantine*, THE ATL. (Apr. 7, 2020), https://www.theatlantic.com/ideas/archive/2020/04/contact-tracing-could-free-america-from-its-quarantine-nightmare/609577/; *see* Shane Harris, *DHS Authorizes Personnel to Collect Information on Protesters It Says Threaten Monuments*, THE WASH. POST (July 20, 2020, 7:27 PM), https://www.washingtonpost.com/national-security/dhs-authorizes-personnel-to-collect-information-on-protesters-it-says-threaten-monuments/2020/07/20/6f58867c-cace-11ea-b0e3-d55bda07d66a_story.html; *cf.* Mark Rumold, *The Playpen Story: Rule 41 and Global Hacking Warrants*, ELEC. FRONTIER FOUND. (Sept. 26, 2016),

VEP protocols and metrics for its decisions should be declassified as much as possible to give the public maximal assurance that the USG is responsibly weighing vulnerabilities with the end goals of both protecting Americans and their information.

To take prophylactic measures against the next "Heartbleed-esque" exploit, and mitigate the requirement to trade on public trust when weighing vulnerabilities, it should be acknowledged that the status quo may be improved by identifying problems with the VEP capable of mitigation and the corresponding solutions. The problems addressed by any legal regime should include the following: a projected increase in vulnerabilities reportable to the VEP, a current regulatory scheme that does not have the force and effect of law, and a current opacity that necessitates an unnecessary trade on public trust. The genesis and iterations of the VEP may serve as a guiding blueprint for offered legal solutions.

B. Increased Reportable Vulnerability Volume

There is likely no silver bullet process for balancing warring operational and public interests in the VEP, but, as stated, there is an ethical imperative to have a process for weighing those interests.[110] It is a threshold DoD goal to have "high-assurance cyber-physical systems"[111] and having a process that mandates inter-agency participation not only aids in vulnerability vetting but also facilitates inter-agency situational awareness and target de-confliction. Technology is being developed to accelerate the discovery of zero-day vulnerabilities across varied software platforms (*e.g.*, COTS, GOTS,

https://www.eff.org/deeplinks/2016/08/illegal-playpen-story-rule-41-and-global-hacking-warrants; *See also* Ambastha, *supra* note 100, at 1-2.

[110] Pell & Finocchiaro, *supra* note 17.

[111] High-assurance cyber-physical systems are systems with adequate safety and security features and are functionally correct. Dr. Raymond Richards, *High-Assurance Cyber Military Systems (HACMS)*, DEF. ADVANCED RSCH. PROJECTS AGENCY, https://www.darpa.mil/program/high-assurance-cyber-military-systems.

Free and Open Source Software) that support military and commercial operations.[112]

An indicator of the upward trend in USG abilities to detect vulnerabilities is the Computer and Humans Exploring Software Security (CHESS) program by the Defense Advanced Research Projects Agency (DARPA) Information Innovation Office (I2O), which strives to create automated cybersecurity analysis strategies that are readily deployable by individuals of a relatively novice technological skill level.[113] By allowing for less skilled persons to find zero-day vulnerabilities accurately and quickly by pairing them with computer software systems, the process of vulnerability discovery becomes more accessible to less skilled hackers, less resource expensive for USG agencies, and more temporally efficient.[114] This program aims to fast-track technological advancements in facilitating zero-day vulnerability analysis so it may secure growing DoD software infrastructure and the progressive integration of software into American PCII.[115] In short, by creating automated vulnerability detection tools that can be used by relatively unsophisticated persons, it becomes possible to "scale vulnerability detection [beyond] current limits."[116] As technology disinhibits access to, or otherwise harnesses techniques used to accomplish tasks associated with vulnerability

[112] *See generally Accelerating Cyber Vulnerability Analysis with Binary Files Rendered as Images*, BATTELLE (2019), https://www.battelle.org/case-studies/case-study-detail/accelerating-cyber-vulnerability-analysis-with-binary-files-rendered-as-images.

[113] DEFENSE ADVANCED RESEARCH PROJECTS AGENCY, BROAD AGENCY ANNOUNCEMENT HR001118S0040 (CHESS) (Apr. 18, 2018) available at https://beta.sam.gov/opp/cb10b80125a2e1377f3920586d36b5c9/view#general.

[114] *Id.* at 5.

[115] *Id.*

[116] Loren Blinde, *DARPA Launches CHESS Program with Industry Day, BAA*, INTELLIGENCE COMMUNITY NEWS (Apr. 23, 2018), https://intelligencecommunitynews.com/darpa-launches-chess-program-with-industry-day-baa/ (quoting Dustin Fraze, program manager of DARPA I2O CHESS program).

discovery,[117] a logical byproduct is an increase in volume of vulnerabilities reportable to the VEP.

Thus, a collateral consequence of the advancements in zero-day vulnerability discovery technology is a projected increase in the volume of vulnerabilities submittable to the VEP. The VEP, a policy conceived during the Bush administration, was calibrated to handle vulnerability processing in an era in which both private and governmental usage of cyber-physical systems was in its infantile stages; the potential for exploits to be used by sophisticated third-party hackers, particularly Advanced Persistent Threat hackers, was marginal, and zero-day vulnerability discovery was a resource-expensive task that required expert, manual labor (this last one being mostly, still true, but growing less so).

Suggested legal solutions for improving the VEP generally include codifying processes that require human deliberation of risk management or monetizing the vendor's risk of disclosure or retention.[118] The idea of so-called "information-markets," where the risk of being attacked in the information domain is monetized, even just within DoD, has been largely vilified in the public square.[119] Moreover, while the notion of codifying the VEP with previously suggested legal frameworks would have a number of benefits, including indicating to the public that the weighing of equities is not done on a purely ad hoc basis, creating a process that requires a human to consider each vulnerability is not feasible given the current and future volume of zero-day vulnerability discoveries.

[117] Tianya Gu et al., *Badnets: Identifying Vulnerabilities in the Machine Learning Model Supply Chain,* IEEE, arXiv:1708.06733v2 (Mar. 11, 2019) available at: https://arxiv.org/pdf/1708.06733.pdf.

[118] Pell & Finocchiaro, *supra* note 17, at 1558; *See also* Kesan & Hayes, *supra* note 11, at 811-12.

[119] In 2004, DARPA proposed the 'Policy Analysis Market' as an information market that would trade in national security matters. The proposal was to create the market solely available within federal agencies. However, the idea was publicly condemned as a future market for terrorist attacks and was characterized by a USG Senator as "morally bankrupt." Kesan & Hayes, *supra* note 11, at 811-12.

The suggestion that solvency may be sought by codifying a VEP that requires human deliberation of each vulnerability[120] fails to address the contemporary aspects of the VEP debate accurately.

C. Reducing Opacity

While the VEP Charter has made the process more public and has provided a report evaluating VEP performance may be sent to Congress,121 much of the VEP remains unclear. Of note, as of 2021, "the public has yet to see a single annual report during the past three years and still [has] no understanding of how the process is working, or if the charter has ever been more than an aspirational document."122 The author reporting this fact reasoned this indicates, "[f]urther steps need to be taken to codify the VEP. It cannot be effective without trust in the process and accountability for the government's activities. The risks that unpatched vulnerabilities pose demand no less."123

The original Daniel blog post argued for the disclosure of the "aggregate numbers of zero-day vulnerabilities discovered, the aggregate numbers of such vulnerabilities disclosed (as opposed to retained for government use), and the length of time that vulnerabilities are kept before disclosure" be disclosed and that disclosure of these details would "not compromise sources and methods of how these vulnerabilities may have been discovered."124 This request remains relevant and may be even more compelling in light of the increased importance of secure software systems and

[120] For example, *see* Pell & Finocchiaro, *supra* note 13, at 1564-72 (suggesting the VEP use, at least in part, a Common Vulnerability Scoring System [CVSSv3] that requires human deliberation to evaluate vulnerabilities submitted to the VEP).
[121] VEP Charter at 5.
[122] Andi Wilson Thompson, *Assessing the Vulnerabilities Equities Process, Three Years After the VEP Charter*, LAWFARE (Jan. 13, 2021, 8:57 AM), https://www.lawfareblog.com/assessing-vulnerabilities-equities-process-three-years-after-vep-charter.
[123] *Id.*
[124] Scwartz & Knake, *supra* note 27, at 2.

continuing examples of vulnerabilities retained by the USG used to effectuate harm (see discussion supra Part II(A)).

The derivative argument for reduced opacity may be cross-applied to prevent the VEP from unnecessarily trading on public trust. The more the VEP is publicized to the world, the more it can justify its decisions, explain its process, and make clear it has not "confused a public relations strategy with a security strategy."125 This would mitigate the problem posed by the Heartbleed vulnerability where the theoretical operational value of retention cannot be publicly balanced against the harm publicly done in-fact. Further, if the metrics for retention are known, the public can more easily understand the justification for retention even if the specifics of the vulnerabilities are unknown. Consequently, the public may be better equipped to trust that retention was purposefully done, carefully considered, and not the product of an arbitrary or uninformed decision. Harm is generally more bearable if it is known that it is borne for good causes.

A specific method of reducing opacity, in addition to publicizing the information encouraged to be publicized by the blog post, is to change the permissive "may" to "must" in the VEP Charter language when it references whether the VEP report should be sent to Congress.126 If it is deemed unfeasible to publicize further VEP details to the public, ensuring Congressional oversight is a first step towards providing an important check on the executive branch's thus-far unilateral decision-making power over whether to retain a vulnerability for law enforcement or operational functions.127

D. Proposed Legal Framework

In the spirit of the original Bush administration directive, the executive branch should again initiate "a joint plan for the

[125] Aitel & Tai, *supra* note 65.

[126] VEP Charter at 5; Under the FAR § 2.101, which contains definitions of terms that govern the FAR and other DoD Regulations, including the DFARS and DGARS where terms are not defined within those documents, "must" and "shall" indicate an imperative.

[127] *See generally* Ghappour, *supra* note 60, at 1132-36

coordination and application of offensive capabilities to defend U.S. information systems."[128] Pursuant to this directive, SMEs from relevant government entities with a stake in the VEP should be directed to structure a VEP legal regime to manage USG interests subsequent to a vulnerability discovery. The SMEs crafting the VEP should strive to ensure USG entities participating in the VEP represent the broad array of interests vested in a high-quality VEP, including entities with law enforcement, intelligence operations, commercial, international partnership, and privacy expertise.

The SMEs should create a VEP plan capable of handling increased vulnerability disclosure and purposed for increased transparency.[129] The directive to create the plan, like the original directive being part of a larger USG-wide effort to promote then-relevant cybersecurity initiatives,[130] should aim to address contemporary issues associated with vulnerability discovery, including the ability for the federal government to potentially increase its rate of discovering vulnerabilities through, for example, human-machine teaming.

Thus, parallel with the original directive, the new directive should be issued with the goal of bringing together SMEs to formulate how best to update the VEP plan to account for new (and old) problems. But primarily, whatever legal structure is created, it should be codified so the legal regime stays in effect regardless of administration change.

Regarding aspects of the legacy VEP plans that may be leveraged going forward, the VEP Charter policies present blueprints for how a VEP may be structured. A positive trait of both the VEP Paper and VEP Charter are the stated policies of disclosure absent a compelling reason to retain. This bias in favor of disclosure should be

[128] Schwartz & Knake, *supra* note 27, at 4.
[129] Schwartz & Knake, *supra* note 27 at 16-17.
[130] *Comprehensive National Cybersecurity Initiative*, NAT'L INST. OF STANDARD AND TECH. (Updated Sept. 26, 2017), https://csrc.nist.gov/Topics/Laws-and-Regulations/executive-documents/CNCI; *See also* Schwartz & Knake, *supra* note 30, at 4.

codified per the discussion in Part II(C). Also, per Part II(C), any codification of the VEP should change the permissive "may" to "must" in reference to whether the VEP Report should be sent to Congress.[131]

Next, the policy in the VEP Charter to generally consider solely coordinated disclosure, and the simplified definitions of "newly discovered" and "publicly known," should be implemented over the alternative definitions and policy of full disclosure offered in the VEP Paper.[132] Not only are the VEP Charter definitions more easily applied, but they capture a greater volume of vulnerabilities.[133] The policy of considering solely coordinated disclosure decreases risk of unnecessarily losing information with inimitable operational value and ensures the primary goal of disclosure remains in assisting vendors in patching vulnerabilities.[134] While there is value to publicizing disclosures openly (*e.g.*, publicizing to lists such as the NVD and the attached benefits of that process that were reviewed at the beginning of the Note),[135] the task of accruing public knowledge for open source usage is secondary to the government's function of creating defensible and secure software and hardware systems. Consequently, the VEP's primary and stated goal should be weighing vulnerabilities for coordinated disclosure.

III. CONCLUSION

In summation, regardless of what law is used, a step towards increased VEP utility requires that law be used. The alternative is leaving the VEP as a notional executive branch policy. A VEP legal regime, created by SMEs in the vulnerability reporting process, should account for increased volume of discovered zero-day vulnerabilities,

[131] VEP Charter at 5.
[132] *C.f.* Johnson, supra note 16, at 1.
[133] *See* discussion in Part I(E)-(F); VEP Paper at 5, 12-13.
[134] *See generally* Hennessey, *supra* note 74; for an example of the positions that full disclosure helps the public, but retention preserves irreplaceable operational value clashing, to the effect of an industry partner revealing zero-days that allegedly shut down a Western counterterrorism operation, *see* Howell O'Neill, *supra*, note 15.
[135] *National Vulnerability Database*, *supra* note 2.

reduce opacity in the VEP, default towards coordinated disclosure, and be enforced through the weight and clarity of statutes.