VIRGINIA JOURNAL OF LAW & TECHNOLOGY

VOLUME 27 SPRING 2024 NUMBER 6

AUDITING THE GOVERNMENT'S VULNERABILITY STOCKPILE

Amy C. Gaudion†

"Building up a huge stockpile of undisclosed vulnerabilities while leaving the Internet vulnerable and the American people unprotected would not be in our national security interest."
Michael Daniel, White House Cybersecurity Coordinator (April 2014)

ABSTRACT

In 2017, the WannaCry and NotPetya attacks wreaked havoc on a global scale, resulting in significant harm to governments, companies, and individuals. Both attacks exploited a software vulnerability found in the Microsoft Windows operating system. The U.S. government had discovered that same vulnerability several years earlier. Rather than notifying Microsoft of the vulnerability, the U.S. government kept the vulnerability secret and used it to develop a set of hacking tools referred to as EternalBlue. These NSA-crafted tools were designed to exploit the vulnerability for intelligence collection and other national security purposes. Unfortunately, the tools landed in the wrong hands, leading to

† Associate Professor of Law, Penn State Dickinson Law. For helpful conversations and commentary on earlier iterations of this project, the author is grateful to Mohamed Rali Badissy, Tiffany Jeffers, Matthew Lawrence, Alison Lintal, Samantha Prince, Laurel Terry, Saurabh Vishnubhakat, Douglas Williams, and Sarah Williams. The author also thanks William Funk, Ronald Lee, Emily McReynolds, David Zaring, and participants at the 2023 Privacy Law Scholars Conference (hosted by the University of Colorado Law School) and the 2023 New Voices in Administrative Law Program (hosted by the AALS Section on Administrative Law) for their insightful observations and feedback. This article benefitted from the terrific research assistance of Jeremy Garica and Maria Germanetti, and from the patience and care of this journal's editors as they shepherded the piece through the editorial process while allowing updates as needed to reflect recent events and ongoing developments. This article reflects developments through early-April 2024, when it was finalized for publication.

the development of the WannaCry and NotPetya malware. These events highlight the equities at stake—and the interests often in collision—when the U.S. government uses vulnerabilities. They also illustrate the risks implicated in the U.S. government's use of cyber-intrusion tools and capabilities, and especially its purchasing, use, and stockpiling of zero-day vulnerabilities. On one side, vulnerabilities are a potent and effective tool, viewed by many governments as indispensable to their intelligence collection, law enforcement, and national security operations. On the other side, critics have lamented the use of vulnerabilities as a shadow tool and have chastised governments for stockpiling vulnerabilities in their cyber arsenals. The critiques are wide-ranging and reflect technical, ethical, policy, and legal dimensions. They question the legality of these cyber stockpiling practices pursuant to traditional frameworks governing constitutional separation of powers and emerging frameworks aimed at recognizing privacy and civil liberties interests in the digital domain. The critiques often lead to calls for codification and increased reporting to legislative bodies and the public.

This article takes a different tact, rejecting the conventional calls for reform. Rather, its thesis is that we should look beyond the traditional oversight players—congressional committees, the judiciary, the media—and consider how oversight from within the executive branch may prove a better match for checking against government overreach, misuse, and abuse. It posits that the auditing tools wielded by the Office of Inspector General of the Intelligence Community (the IC IG), as well as other features of that office, provide a more suitable fit for the government activity in need of oversight when that activity relies on vulnerabilities and other cyber-intrusion capabilities.

Part I offers a primer on how governments use vulnerabilities, and the decision-making frameworks governments use when assessing which vulnerabilities to disclose and which to retain for offensive purposes. This part then explores the U.S. VEP's origins, its structures and processes, and its interaction with other efforts designed to encourage information sharing and collaboration with the private sector. It also considers how recent developments domestically and internationally may be reshaping the U.S. VEP and governmental use of vulnerabilities. Part II describes the existing domestic legal authorities and oversight mechanisms that guide the U.S. government's use of vulnerabilities. This part examines the failure of early congressional efforts to codify the U.S. VEP's review process and the subsequent shift to reporting requirements. It flags shortcomings in the statutory reporting requirements and catalogs lingering

concerns about the U.S. VEP's ability to appropriately reflect and weigh the interests of affected stakeholders. Part III considers the oversight landscape from within the executive branch, and proposes an expanded role for the office of the IC IG. The article concludes by illustrating how the IC IG can wield its auditing and other tools to kickstart reform efforts. An IC IG audit of the government's vulnerability stockpile creates a channel for checking governmental power, correcting abuses, and protecting privacy and civil liberties interests in the digital domain; aligns the government's use of vulnerabilities for legitimate purposes with its efforts to achieve effective private-sector collaboration; and reorients the U.S. government's conduct to reflect evolving norms of responsible behavior in cyberspace.

INTRODUCTION

In the spring of 2017, the WannaCry attack, later attributed to North Korea, and the NotPetya attack, later attributed to Russia, wreaked havoc on a global scale and caused the loss of billions of dollars for governments and private companies. Both attacks exploited a software vulnerability found in the Microsoft Windows operating system. The U.S. government had discovered that same vulnerability several years earlier. Rather than notifying Microsoft of the vulnerability, the U.S. government kept the vulnerability secret and used it to develop a set of hacking tools referred to as EternalBlue.[1] These NSA-crafted tools were designed to exploit the vulnerability for intelligence collection and other national security purposes.[2] These were no ordinary hacking tools; indeed, reports have described them as the most effective and potent tools in the government's vulnerability arsenal.[3] Despite the U.S. government's efforts to keep the vulnerability and the tools secret, they were desired by cyber actors outside the U.S. government. In early 2017, the EternalBlue hacking tools were leaked by a group known as Shadow Brokers, and led to the development of WannaCry, NotPetya, and other copycat malware.[4] When the U.S. government's decision to retain the EternalBlue vulnerability became public, the news stories were less than flattering. A May

---

[1] 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/.

[2] *Id.* For a detailed history of this episode, see BEN BUCHANAN, THE HACKER AND THE STATE: CYBER ATTACKS AND THE NEW NORMAL OF GEOPOLITICS 253–54 (2020); ANDY GREENBERG, SANDWORM: A NEW ERA IN CYBERWAR AND THE HUNT FOR THE KREMLIN'S MOST DANGEROUS HACKERS 164–65, 182–83 (2020); and NICOLE PERLROTH, THIS IS HOW THEY TELL ME THE WORLD ENDS: THE CYBER WEAPONS ARMS RACE 308–09, 340–41, 347–49 (2020). Neither the NSA nor any other entity of the U.S. government has officially acknowledged the government's role in developing or use of EternalBlue. Other media and industry sources—including Microsoft—however, have concluded that the hacking tools in the EternalBlue family have NSA origins. 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://bit.ly/49r8h7e; Newman, *supra* note 1; PERLROTH, *supra*, at 308-309.

[3] *EternalBlue Exploit: What It Is and How It Works*, SENTINELONE (May 17, 2019), https://bit.ly/42xNKM2; *see also supra* note 2 and sources cited therein.

[4] Newman, *supra* note 1. For an earlier glimpse of the Shadow Brokers' efforts to steal NSA-designed hacking tools, see Andy Greenberg, *The Shadow Brokers Mess Is What Happens When the NSA Hoards Zero-Days*, WIRED (Aug. 17, 2016), https://www.wired.com/2016/08/shadow-brokers-mess-happens-nsa-hoards-zero-days/#:~:text=8%3A34%20PM-,The%20Shadow%20Brokers%20Mess%20Is%20What%20Happens%20When%20the%20NSA,the%20agency's%20controversial%20hacking%20activities (describing pitfalls when the NSA's "secret hacking tools can fall into unknown hands").

2017 article in Forbes proclaimed that "An NSA Cyber Weapon Might Be Behind A Massive Global Ransomware Outbreak" and a March 2018 headline in Wired Magazine described "The Leaked NSA Spy Tool that Hacked the World."[5]

The EternalBlue case study highlights the trade-offs implicated in the U.S. government's use of cyber-intrusion tools and capabilities, and especially its purchasing, use, and stockpiling[6] of zero-day vulnerabilities. A "vulnerability" is "a weakness in an information system or its components (for example, system security procedures, hardware design, and internal controls) that could be exploited or could affect confidentiality, integrity, or availability of information."[7] Zero-day vulnerabilities—or "0-days"—are particularly effective tools, and refer to a previously unknown "software or hardware flaw for which there is no existing patch."[8] They are so named because once discovered, they may be used immediately to gain access, and they give the developer zero days to issue a patch or otherwise mitigate the damage of the exploit.[9]

---

[5] Newman, *supra* note 1; Thomas Brewster, *An NSA Cyber Weapon Might Be Behind A Massive Global Ransomware Outbreak*, FORBES (May 12, 2017), https://bit.ly/42wbErj.

[6] Stockpiling may be an odd word choice because it implies that items (in this case vulnerabilities) are sitting in a warehouse, waiting to be used. In contrast to traditional kinetic weapons, vulnerabilities are likely better described as "raspberries—they go bad fast." Dakota Cary & Kristin Del Rosso, *Sleight of Hand: How China Weaponizes Software Vulnerabilities*, ATL. COUNCIL REP. (Sept. 6, 2023), https://bit.ly/3uzfcfK. Nonetheless, the label stuck and seems an appropriate fit as it captures the concerns about government retention and the idea that governments are engaging in the gathering and storage of these tools anticipating their use at a later time.

[7] 50 U.S.C. § 3316a(a)(3). Similar definitions of vulnerability can be found in industry and international sources. *See* GOOGLE THREAT ANALYSIS GROUP (TAG), BUYING SPYING: INSIGHTS INTO COMMERCIAL SURVEILLANCE VENDORS 14 (2024) [hereinafter GOOGLE TAG, BUYING SPYING] (defining vulnerability as a "weakness in a device or software that can be exploited to gain access or to perform unauthorized actions on the system."); *The Pall Mall Process: Tackling the Proliferation and Irresponsible Use of Commercial Cyber Intrusion Capabilities*, MINISTRY FOR EUR. AND FOREIGN AFFS., https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/news/article/the-pall-mall-process-tackling-the-proliferation-and-irresponsible-use-of (last visited Apr. 13, 2024) [hereinafter *Pall Mall Process*] ("A vulnerability is a weakness, or flaw, in a system or process. An attacker may seek to exploit a vulnerability to gain access to a system. The code developed to do this is known as an exploit.").

[8] PERLROTH, *supra* note 2, at 7.

[9] THE VULNERABILITIES EQUITIES POLICY AND PROCESS FOR THE U.S. GOVERNMENT, Annex A (2017), bit.ly/3uJh4mv [hereinafter U.S. VEP]; *see also* GOOGLE TAG, BUYING SPYING, *supra* note 7, at 14–15 (defining "0-day exploit" as "An exploit that uses a vulnerability that defenders do not yet know exists. There is no security patch available to prevent exploitation, nor antivirus signatures that can detect exploitation."); *Pall Mall Process*, *supra* note 7 ("A zero-day exploit exploits a vulnerability where there are no security fixes yet available. A zero-day vulnerability becomes an n-day vulnerability once a security fix (patch) has been issued by the vendor.").

The WannaCry and NotPetya events illustrate the equities at stake—and the interests often in collision—when the government uses vulnerabilities. On one side, vulnerabilities are an effective tool to counter encryption and a potentially desirable alternative to insisting on "exceptional access" or backdoors for government entities.[10] Most commentators, though not all, view their use as indispensable to intelligence collection, law enforcement, and national security operations.[11] The potency of such tools and their increasing use by nation-state adversaries and non-state actors lead many to conclude that the U.S. government's use of vulnerabilities is here to stay.[12] On the other side,

---

[10] Alan Rozenshtein, *Wicked Crypto*, 9 U.C. IRVINE L. REV. 1181, 1207 (2019) [hereinafter Rozenshtein, *Wicked*] ("The biggest argument in favor of lawful hacking is that it takes advantage of pre-existing vulnerabilities in computer and communications systems. Unlike exceptional-access mandates, lawful hacking does not require providers to make changes to their systems that might introduce even more security flaws.")

[11] *See* CYBER THREAT ALLIANCE & CENTER FOR CYBERSECURITY POLICY & LAW, MORE SUNLIGHT, FEWER SHADOWS: GUIDELINES FOR ESTABLISHING & STRENGTHENING GOVERNMENT VULNERABILITY DISCLOSURE POLICIES 3 (2021) ("[G]overnments have legitimate interest in pursuing national security and law enforcement goals through the use of vulnerabilities because they can use those holes to identify and catch malicious actors and help to keep people safe.") [hereinafter MORE SUNLIGHT]; Sven Herpig & Ari Schwartz, *The Future of Vulnerabilities Equities Processes Around the World*, LAWFARE (Jan. 4, 2019), https://www.lawfaremedia.org /article/future-vulnerabilities-equities-processes-around-world ("As more information becomes encrypted in transit, governments have a greater need to access information by hacking the end points of the communications. Yet, even with proper legal process, a government may need to utilize new exploits or try to hold on to otherwise unknown exploits in their hacking efforts."). *But cf.* David Kaye & Sarah McKune, *The Scourge of Commercial Spyware—and How to Stop It*, LAWFARE (Aug. 25, 2023), https://www.lawfaremedia.org /article/the-scourge-of-commercial-spyware-and-how-to-stop-it (questioning assertion that commercial spyware and lawful hacking are necessary tools, and proposing more robust interrogation of claims that spyware and lawful hacking are "essential" government tools); JULIET SKINGSLEY, OFFENSIVE CYBER OPERATIONS: STATES PERCEPTIONS OF THEIR UTILITY AND RISKS, CHATHAM HOUSE, 26–30 (2023) (calling for a "more nuanced understanding of the utility and value of offensive cyber capabilities" questioning whether utility is well understood, and doubting that deterrence is as effective as often claimed).

[12] *See* Dina Temple-Raston, *The Nature of Bug Bounty Programs Is Changing, and Their 'Auntie' Is Worried (Interview of Katie Moussouris)*, THE RECORD (Jan. 12, 2024), https://therecord.media/katie-moussouris-vulnerability-disclosure-china-european-union?utm_medium=email&_hsmi=289995689&utm_content=289995689&utm_source=hs_email ("And I think the concern here is that other adversarial governments can use these things against, in our case, the U.S. and our allies. So everybody wants in on it."); *see also* Asaf Lubin, *Regulating Commercial Spyware*, THE DIGITAL SOCIAL CONTRACT: A LAWFARE PAPER SERIES, Aug. 2023, at 36 ("So we need to accept that spyware is here to stay."). For descriptions of the role vulnerabilities play in various government operations, see Robert M. Chesney, *The Domestic Legal Framework for US Military Cyber Operations*, *in* THE UNITED STATES' DEFEND FORWARD CYBER STRATEGY: A COMPREHENSIVE LEGAL ASSESSMENT 67–70 (Jack Goldsmith ed., 2022) (use of vulnerabilities in military offensive cyber operations); Lubin, at 36 (use of vulnerabilities in commercial spyware); Rozenshtein, *Wicked,*

critics have lamented the use of vulnerabilities as a shadow tool and others have chastised governments for stockpiling vulnerabilities in their cyber arsenals. The critiques fall into several categories, most notably their awkward fit with the public law values of accountability and transparency, their tendency to undercut efforts at information sharing and operational collaboration between government and industry, their violation of the privacy interests of consumers, their adverse impact on the development of norms of responsible behavior in cyberspace, and the harm caused to the interests of the public and industry in the establishment and availability of a secure internet.[13]

Despite calls from Microsoft CEO Brad Smith and others to require governments "to report vulnerabilities to vendors, rather than stockpile, sell, or exploit them,"[14] the decision to retain a vulnerability for governmental use is not expressly prohibited under current domestic or international legal frameworks.[15] Instead, such decisions are governed by internal governmental processes that seek to balance the complicated dynamics and competing interests at stake.[16] In engaging the difficult question of vulnerability disclosure,

---

supra note 10, at 1207 (use of vulnerabilities in lawful hacking operations by law enforcement and intelligence entities).

[13] Practitioners and scholars have acknowledged the legitimacy, value, and utility of vulnerability-enabled tools while expressing concern about potential government overuse and abuse of such capabilities. While governments use vulnerabilities "to achieve important law enforcement, public safety, and national security goals" the "risks posed by government mishandling or misuse are significant and as government hacking grows ever more common, each new, unfixed vulnerability represents a potential risk to a variety of national interests." MORE SUNLIGHT, *supra* note 11, at 4. *See infra* Section II.C describing concerns and critiques of governmental vulnerability use and the U.S. vulnerability disclosure process.

[14] Smith, *supra* note 2.

[15] While the existing legal architecture does not expressly prohibit the use of vulnerabilities or the government's decision to retain a vulnerability for exploitation in its operations, evolving international norms arguably call the practice into some question. *See, e.g.*, Rep. of the Grp. of Governmental Experts on Devs. in the Field of Info. and Telecomms. in the Context of Int'l Sec., U.N. Doc. A/70/174, at 13(j) (2015) (proposing norms of responsible behavior in cyberspace, including that states should encourage "responsible reporting of ICT vulnerabilities and share associated information on available remedies to such vulnerabilities to limit and possibly eliminate potential threats to ICTs and ICT dependent infrastructure"). Indeed, the lack of express prohibitions on the use of vulnerabilities forms the basis for reform recommendations sounding in both domestic and international law. *See generally* Kaye & McKune, *supra* note 11; SKINGSLEY, *supra* note 11.

[16] Authors Sven Herpig and Ari Schwartz, who both served as former government officials, offer a helpful description of the "difficult dilemma" facing governments regarding the use of vulnerabilities:

> Governments are simultaneously charged with helping protecting [*sic*] the public from exploits online, on the one hand, and with intelligence, law enforcement and military missions that may require the use of such

the U.S. government relies on an executive branch policy called the Vulnerabilities Equities Policy and Process (U.S. VEP), which weighs the benefits of sharing vulnerability information with industry and the public against the need to retain it for legitimate national security, intelligence, or law enforcement purposes.[17]

The U.S. government, of course, is not the only state that relies on vulnerabilities, and particularly zero-day vulnerabilities, to accomplish national security, intelligence, and law enforcement objectives. Indeed, these tools are generally recognized as necessary components in a government's cyber arsenal.[18] Their use, however, creates two significant challenges. First, a government's decision to retain, and thus not disclose certain vulnerabilities to industry or the public, may create a "boomerang effect" or "friendly fire" problem whereby the very same cyber tools utilized by that government for a national security purpose come back to wallop companies and individuals in that country, and even other government agencies.[19] The problem of

> vulnerabilities, on the other. A decision to retain a zero day vulnerability likely undercuts the cybersecurity of the public, enterprises and even government agencies. But disclosing information about a zero day vulnerability so vendors can patch it risks undercutting the ability of law enforcement to investigate crimes, intelligence agencies to gather intelligence, and the military to carry out offensive cyber operations.

Herpig & Schwartz, *supra* note 11. For a discussion of government vulnerability disclosure processes as well as other types of vulnerabilities disclosure process, see *infra* notes 24–32 and accompanying text.

[17] U.S. VEP, *supra* note 9.

[18] *See, e.g.*, U.S. DEP'T OF DEF., 2023 CYBER STRATEGY OF THE DEPARTMENT OF DEFENSE SUMMARY 2 (2023) ("[C]yberspace operations represent an indispensable element of U.S. and Allied military strength and form a core component of integrated deterrence."); *see also supra* notes 11 and 12 and sources cited therein (describing appeal and staying power of governmental vulnerability-based intrusion capabilities). While the nations with the most developed and well-known cyber arsenals continue to be U.S., Russia, China, Iran, and North Korea, the "number of governments with offensive cyber capabilities has been growing as the relevance of cyberspace as a domain of geopolitical conflict has become increasingly apparent." MORE SUNLIGHT, *supra* note 11, at 7. A 2021 report, prepared by the Cyber Threat Alliance and the Center for Cybersecurity Policy and the Law, identified the following EU countries as "leveraging these zero-day vulnerabilities" in their governments' offensive cyber capabilities: Germany, France, Italy, Hungary, Luxembourg, Czechia, Spain, Cyprus and Poland. *Id.* A more recent 2024 report identified the sale of "hacking software," which relies on vulnerabilities and other cyber-intrusion technology, to the following countries: Egypt, Armenia, Greece, Madagascar, Côte d'Ivoire, Serbia, Spain, and Indonesia. GOOGLE TAG, BUYING SPYING, *supra* note 7, at 13.

[19] PERLROTH, *supra* note 2, at 308–09, 347–49 (describing "boomerang effect"). Katie Moussouris, founder and CEO of Luta Security, labels this the "friendly fire" problem and explains that "[w]e haven't gotten our head around the fact that keeping vulnerability information in order to exploit it has a much higher chance of backfiring than any government really wants

unintended consequences is not new or particularly novel, but it is worth noting as it provides context for appreciating the second challenge. It is the second challenge that is the focus of this article: the "stealthy features" that necessarily characterize vulnerability-enabled capabilities evade the usual checking mechanisms, casting doubt on their alignment with democratic norms of accountability and transparency.[20] As a result, the use of vulnerabilities by the U.S. and other governments has been the focus of considerable commentary.

---

to admit." Temple-Raston, *supra* note 12. "If we cannot adapt ourselves to that idea, we are going to see more and more of these friendly fire escapes that cripple the world." *Id.*

[20] Jack Goldsmith & Matthew Waxman, *The Legal Legacy of Light-Footprint Warfare*, 39 WASH. Q. 7, 18 (2016) (describing how light footprint warfare, including through the use of cyber-intrusion tools, may be a "bug for U.S. democracy, since the stealthy features mean that public debate and political checks—which reduce error as well as excess, and promote legitimacy—function ineffectively"). As with many other national security tools, particularly those that are vulnerability-enabled, the use of such technologies and tools by governments pushes against the norms of democracy and accountability creating oversight obstacles and challenges in the traditional checks and balances framework. *See* New York Times Co. v. United States, 403 U.S. 713, 727–728 (1971) (Stewart, J., concurring) ("In the governmental structure created by our Constitution, the Executive is endowed with enormous power in the two related areas of national defense and international relations. This power, largely unchecked by the Legislative and Judicial branches, has been pressed to the very hilt since the advent of the nuclear missile age."); DANIEL BYMAN, DANIEL W. LINNA JR. & V. S. SUBRAHMANIAN, GOVERNMENT USE OF DEEPFAKES: THE QUESTIONS TO ASK, CTR FOR STRATEGIC & INT'L STUD. 1 (2024) ("This proliferation of AI provides an unparalleled opportunity for state actors to use deepfakes for national security purposes."); Rebecca Crootof, *Autonomous Weapons and the Limits of Analogy*, 9 HARV. NAT'L SEC. J. 51, 82–83 (2018) (describing challenges of applying existing legal frameworks to emerging weapon technologies, noting that "[w]hile analogical reasoning allows 'most law-of-war rules [to] apply most of the time to most new technologies,' in some situations there is no way to credibly stretch existing rules to answer novel legal questions.") (quoting Kristen E. Eichensehr, *Cyberwar and International Law Step Zero,* 50 TEX. INT'L L.J. 357, 359 (2015)); Ashley Deeks, *Will Cyber Autonomy Undercut Democratic Accountability?*, 96 INT'L L. STUD. 464, 465–66 (2020) (describing how cyber operations could alter existing relationships between the legislative and executive branches because they "are harder to detect publicly and do not require the type of robust legislative support that large-scale conflicts do"); Timothy Edgar, *Recent Botnet Takedowns Allow U.S. Government to Reach Into Private Devices*, LAWFARE (Mar. 13, 2024), https://www.lawfaremedia.org/article/recent-botnet-takedowns-allow-u.s.-government-to-reach-into-private-devices (urging Congress to reject use of nationwide hacking warrants "in favor of an alternative legal framework that authorizes domestic cybersecurity operations to remediate botnets and other malware in carefully circumscribed situations, with more thorough review and oversight by the courts"), Elad D. Gil, *Cyber Checks and Balances*, 54 CORNELL INT'L L.J. 101, 105–07 (2021) (explaining need for "exogenous forces and actors" beyond the judicial and legislative branches to "constrain and empower the government in the digital sphere, thereby affording a better understating of how the cyber separation of powers works in practice."); Jason Healey, *Soldiers, Statesmen and Cyber Crises: Cyberspace and Civil-Military Relations*, LAWFARE (Mar. 16, 2022), https://www.lawfaremedia.org/article/soldiers-statesmen-and-cyber-crises-cyberspace-and-civil-military-relations ("Cyber conflict is not only a 'persistent engagement' taking place in this gray zone, but it will also have no end: '[S]uperiority in cyberspace is temporary,' in the words of

Scholars, journalists and former government officials have examined this subject, recording the competing interests at stake, assessing the governing legal and policy frameworks—or noting the lack thereof—and measuring the consequences of vulnerability-enabled operations by governments, both anticipated and unintended.[21] They have questioned the legality of cyber stockpiling practices while calling for greater transparency and more rigorous oversight, usually by proposing codification and increased reporting to legislative bodies and the public. This article takes a different tact, rejecting the conventional calls for reform. Rather, its thesis is that we should look beyond the traditional oversight players—congressional committees, the judiciary, the media—and shift perspectives to consider how oversight from within the executive branch may prove a better match for checking against government overreach, misuse, and abuse. It posits that the auditing tools wielded by the inspector general of the intelligence community, as well as other features of the position, provide a more suitable fit for the government activity in need of oversight when that activity relies on vulnerabilities and other cyber-intrusion capabilities.

Part I examines the government's use of vulnerabilities and explores the U.S. VEP's origins in the wake of 9/11 and its subsequent formal acknowledgment, structures and processes, and interaction with other efforts

---

Gen. Paul M. Nakasone, the commander of U.S. Cyber Command."); Benjamin Jensen & J.D. Work, *Cyber Civil-Military Relations: Balancing Interests on the Digital Frontier*, WAR ON THE ROCKS (Sept. 4, 2018), https://warontherocks.com/2018/09/cyber-civil-military-relations-balancing-interests-on-the-digital-frontier/ (describing concerns that empowering "Cyber Command to conduct short-notice attacks without White House approval or interagency coordination" will work a dramatic shift in civil-military relations leading to "a professional military cyber force capable of autonomously protecting society absent constant civilian oversight."); SKINGSLEY, *supra* note 11, at 29. ("The invisibility of cyber activity is all the more reason for robust independent oversight of these activities."); Matthew C. Waxman, *Cyberattacks and the Constitution*, HOOVER INST., 11 (Nov. 11, 2020), https://bit.ly/3STWuZU (questioning whether cyber operations form a "new constitutional category altogether, for which the respective roles of Congress and the president are not yet established.").

[21] *See generally* the following sources at note 2 (BUCHANAN; GREENBERG; PERLROTH); Cary & Del Rosso, *supra* note 6; Denelle Dixon, *WannaCry Is a Cry for VEP Reform*, MOZILLA BLOG (May 15, 2017), https://mzl.la/499Vq9V; Herpig & Schwartz, *supra* note 11; Kaye & McKune, *supra* note 11; Jason Healey, *The U.S. Government and Zero-Day Vulnerabilities: From Pre-Heartbleed to Shadow Brokers*, COLUM. J. OF INT'L AFF. (Nov. 1, 2016), https://microsoft.com/en-us/security/business/microsoft-digital-defense-report-2022 [hereinafter Healey, *Zero-Day Vulnerabilities*]; MICROSOFT DIGITAL DEFENSE REPORT (2022) [hereinafter MICROSOFT REPORT 2022]; SKINGSLEY, *supra* note 11; Smith, *supra* note 2; YUAN STEVENS, STEPHANIE TRAN, RYAN ATKINSON & SAM ANDREY, SEE SOMETHING, SAY SOMETHING: COORDINATING THE DISCLOSURE OF SECURITY VULNERABILITIES IN CANADA, CYBERSECURE POLICY EXCHANGE 44 (2021) [hereinafter SEE SOMETHING, SAY SOMETHING]. *See also infra* Section II.C and accompanying notes describing lingering concerns and challenges to the U.S. government's use of vulnerabilities.

designed to encourage information sharing and collaboration with the private sector. This part identifies the key agency players and analyzes the decision-making structure and the discovery-to-decision timeline. It explains the vulnerability identification and equity assessment processes, taking particular note of the policy's exceptions and exclusions, including those vulnerabilities that fall outside the U.S. VEP's parameters. In addition, it explores how the U.S. VEP interacts with other vulnerability disclosure policies and cyber information sharing initiatives, including with private sector entities and foreign partners. It also considers how recent developments domestically and internationally may be reshaping the U.S. VEP and governmental use of vulnerabilities.

Part II describes the existing domestic legal authorities and oversight mechanisms that guide the U.S. government's use of vulnerabilities. This part examines the failure of early congressional efforts to codify the U.S. VEP's review process and the subsequent shift to reporting requirements. It focuses specific attention on the congressional reporting framework established in the National Defense Authorization Act for Fiscal Year 2020, and embedded Intelligence Authorizations for Fiscal Years 2018, 2019, and 2020. This part concludes by flagging shortcomings in the statutory reporting requirements and cataloging lingering concerns about the U.S. VEP's ability to appropriately reflect and weigh the interests of affected stakeholders. Recognizing the wide scope of such criticism,[22] spanning technical, ethical, policy, and legal dimensions, this part highlights those critiques that impact oversight and

[22] *See generally* Tristian Caulfield, Christos Ioannidis & David Pym, *The U.S. Vulnerabilities Equities Process: An Economic Perspective, in* DECISION AND GAME THEORY FOR SECURITY (Stefan Rass et al. eds., 2017); Sharon Bradford Franklin, *The Need for Countries to Establish Robust and Transparent Vulnerabilities Equities Processes*, 6 FLETCHER SEC. REV. 46 (2019); SVEN HERPIG, GOVERNMENTAL VULNERABILITY ASSESSMENT AND MANAGEMENT: WEIGHING TEMPORARY RETENTION VERSUS IMMEDIATE DISCLOSURE OF 0-DAY VULNERABILITIES 1 (2018) [hereinafter HERPIG, WEIGHING]; Herpig & Schwartz, *supra* note 11; Amy C. Gaudion, *It's Time to Reform the U.S. Vulnerabilities Equities Process,* WAR ROOM BLOG (Sept. 2, 2021), https://warroom.armywarcollege.edu/articles/vep/; Stephanie Pell, *The Ethical Imperative for a Vulnerability Equities Process and How the Common Vulnerability Scoring System Can Aid that Process*, 49 CONN. L. REV. 1549 (2017); Lindsey Polley, To Disclose or Not to Disclose, That Is the Question: A Methods-Based Approach for Examining & Improving the US Government's Vulnerabilities Equities Process (Mar. 2022) (Ph.D. dissertation, Pardee RAND Graduate School), https://www.rand.org/pubs/rgs_dissertations/RGSDA1954-1.html; Michelle Richardson, *Locking in Transparency on the Vulnerabilities Review Process*, JUST SEC. (July 27, 2018), https://bit.ly/49dKZlB; ARI SCHWARTZ & ROB KNAKE, GOVERNMENT'S ROLE IN VULNERABILITY DISCLOSURE: CREATING A PERMANENT AND ACCOUNTABLE VULNERABILITY EQUITIES PROCESS , THE CYBERSECURITY PROJECT AT THE HARV. KENNEDY SCH. BELFER CTR 1 (2016) [hereinafter SCHWARTZ & KNAKE]; Andi Wilson Thompson, *Assessing the Vulnerabilities Equities Process, Three Years after the VEP Charter*, LAWFARE (Jan. 13, 2021), https://bit.ly/3iIFUwE.

accountability. The U.S. VEP (1) lacks key players and perspectives in its decision-making process; (2) excludes a wide swath of vulnerabilities from any review under the U.S. VEP's "exceptions" and "exclusions" provisions; (3) lacks consistent agency interpretations and processes for defining and identifying vulnerabilities that require submission to the U.S. VEP; (4) is inconsistent with industry disclosure standards and information sharing expectations; and (5) lacks an enforcement or accountability mechanism to assess whether the process is being followed and to impose consequences for non-compliance.

Part III considers the oversight landscape from within the executive branch. It explains the need for a new player in the vulnerability oversight game, one able to balance the U.S. government's need for flexibility in the use of vulnerabilities with calls for independent and vigorous oversight. This part then proposes a role for the Office of the Intelligence Community Inspector General ("IC IG"). It explains why the work of internal oversight entities, like the IC IG, is necessary when the governmental activity relies on rapid technological advances and its operational effectiveness requires speed and secrecy. This part first examines the attributes of inspectors general in the U.S. constitutional scheme, and then profiles the IC IG's specific tools and partners in relation to the vulnerability oversight task. It considers how the Office of the IC IG can wield its tools to kickstart reform efforts, focused on more effectively aligning the U.S. government's use of vulnerabilities for legitimate purposes with its efforts to achieve cyber-related collaboration with the private sector and to be a leader in the development of cyber norms. Prioritizing the work of these unconventional and often overlooked mechanisms in the oversight ecosystem will appropriately align the government's use of vulnerabilities for legitimate purposes with efforts to check governmental power, correct abuses, and protect privacy and civil liberties interests in a complicated cyber domain.

I. A PRIMER ON VULNERABILITIES, VULNERABILITY DISCLOSURE PROCESSES, AND THE U.S. VULNERABILITIES EQUITIES POLICY & PROCESS

As noted above, the U.S. government's decision to retain the EternalBlue vulnerability was denounced by privacy advocates, scholars, industry leaders, and foreign partners. However, no U.S. law expressly prohibited the government's decision to keep the vulnerability secret. Rather, in making these decisions governments rely on internal decision-making processes. The objective of such processes is to establish frameworks and criteria for deciding whether to retain or disclose newly discovered vulnerabilities, or take some

action between full retention and full disclosure. The process should be structured to appropriately consider and weigh competing interests, including those of the public, industry, as well as government entities with conflicting perspectives (from the agencies representing defense, intelligence, and law enforcement assessments to those reflecting economic and diplomatic concerns). Achieving these objectives is no easy task. However, given the importance of these cyber tools and their uncomfortable fit with democratic norms, the need for such processes is apparent.

This section provides an introductory primer[23] on the U.S. government's vulnerability decision-making structure: the U.S. VEP. This section provides an overview of how the U.S. VEP fits into the larger vulnerability disclosure and cyber information sharing landscape. It identifies the key players in the decision-making structure and describes the vulnerability identification and equity assessment processes. It points out the policy's exceptions and exclusions, including those vulnerabilities that fall outside the U.S. VEP's parameters. It considers the U.S. VEP's interaction with other vulnerability disclosure efforts, including those of other government entities, industry, and foreign partners. It also considers domestic and international legal developments that may impact the use of cyber-intrusion and vulnerability-enabled capabilities. It concludes by considering how the EternalBlue case study profiled above would have worked its way through the U.S. VEP.

Where does the U.S. VEP fit in the vulnerability disclosure framework and the larger cyber information-sharing landscape?

Let's start by considering what we mean by "vulnerability disclosure." The term is best defined as "[p]roviding information on a vulnerability to a party that is likely unaware of it,"[24] and is a helpful way to think about the different

[23] This section is designed to provide a brief primer on the U.S. VEP, highlighting the actors and mechanisms needed to understand the critiques and proposed solutions in this article. For a comprehensive treatment of the U.S. VEP, see generally Healey, *Zero-Day Vulnerabilities, supra* note 21; Polley, *supra* note 22; SCHWARTZ & KNAKE, *supra* note 22.

[24] SEE SOMETHING, SAY SOMETHING, *supra* note 21, at 44 (referencing the standardization and definition efforts of the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), and incorporating definition sections in ISO/IEC 29147:2018, https://www.iso.org/obp/ui/es/#iso:std:iso-iec:29147:ed-2:v1:en). The range of disclosure options for the discovering entity include no disclosure (where knowledge of the vulnerability is kept secret and retained by the discovering entity), coordinated disclosure effort (where discovering entity works together with other entities to ensure disclosure occurs in a way that limits risk), limited or partial disclosure (where some, but not all, of the information known about the vulnerability is disclosed publicly, or is disclosed to some, but not all, affected parties), and full disclosure (all information is released to the public). *Id.* (citations omitted).

categories of disclosure policy. The categories will depend on who the entity is that discovers or has knowledge of the vulnerability and who the party is that is unaware of the vulnerability and likely will be subject to the consequences if the vulnerability is exploited.

The first category governs instances when the government is the entity that discovers or has knowledge of a vulnerability. These policies are often called Government Vulnerability Disclosure (GVD) policies, Vulnerability Equities Processes (VEPs), or Governmental Disclosure Decision Processes (GDDPs). The focus of this article, the U.S. VEP, falls into this category. These are "internal policymaking structures"[25] that describe the processes that governments follow when deciding whether to disclose or retain knowledge of a vulnerability in order to exploit it for law enforcement, national security, or intelligence purposes.[26] Others have described these structures more bluntly, as a pro and con weighing process where the government asks "[w]hat kind of damage would this do to our critical infrastructure and private industry if we kept this [vulnerability] a secret?"[27] While the goal of such policies is to balance the interests of government, industry, and the public, the decision-making structures tend to include only government agencies, and rarely, if ever, involve non-governmental entities from industry or civil society groups.

A different set of motives and criteria govern when the entity discovering the vulnerability is from outside government – most often from the security researcher community. The labels for this second group include Vulnerability Disclosure Policies (VDPs) or Coordinated Vulnerability Disclosure (CVD) policies. These policies have been adopted by a variety of organizations, including governments and industry, to "facilitate the reporting of vulnerabilities in those organizations' systems and networks" when the

---

[25] MORE SUNLIGHT, *supra* note 11, at 5 (defining Government Vulnerability Disclosure (GVD) as "internal policymaking structures that governments need to implement in order to adequately assess and weigh the potential costs and benefits of immediately disclosing knowledge of previously unidentified cybersecurity vulnerabilities, versus retaining that knowledge based upon carefully considered and time-limited justifications.").

[26] *See id. See also* CENTRE FOR EUROPEAN POLICY STUDIES (CEPS), SOFTWARE VULNERABILITY DISCLOSURE IN EUROPE: TECHNOLOGY, POLICIES AND LEGAL CHALLENGES 63 (2018) [hereinafter CEPS, VULNERABILITY DISCLOSURE IN EUROPE] (describing GDDP as a process for "how governments make decisions about how and whether to disclose a vulnerability immediately or to delay disclosure"); Herpig & Schwartz, *supra* note 11 (explaining that government disclosure decision process (GDDP) is the "European umbrella term for VEP"). Some researchers distinguish between the types of government policy relating to vulnerabilities, separating policies relating to vulnerability "disclosure" from those relating to the "acquisition" and "exploitation" of vulnerabilities. CEPS, VULNERABILITY DISCLOSURE IN EUROPE, *supra*, at 63.

[27] Temple-Raston, *supra* note 12.

disclosing entity is a security researcher.[28] For example, the U.S. government uses such policies to provide a channel for security researchers and others to share vulnerability information and report security flaws "in government IT systems to the relevant federal agencies without fear of reprisal for 'hacking' into a government system."[29] Unlike GDDPs or VEPs, these policies provide a framework "where disclosers and organizations work in cooperation to examine and resolve discovered vulnerabilities."[30] They typically involve "reporting, coordinating, and publishing information about a vulnerability and its resolution" with the aim of ensuring resolution and limiting risk.[31] The principles that underly CVDs and VDPs include reducing harm, presuming benevolence of the part of individuals who report vulnerabilities, avoiding surprise by keeping key stakeholders "in the loop," and incentivizing cooperative behavior.[32]

---

[28] MORE SUNLIGHT, *supra* note 11, at 5.

[29] Josh Kenway & Michael Garcia, *To Patch or Not to Patch: Improving the US Vulnerabilities Equities Process*, THIRD WAY (June 1, 2021), https://www.thirdway.org/memo/to-patch-or-not-to-patch-improving-the-us-vulnerabilities-equities-process. The authors explain how the U.S. government's VDPs or CVD policies are distinct from the U.S. VEP's mechanism. *Id. See also* CHRIS JAIKARAN, CONG. RSCH. SERV., IN11497, CYBERSECURITY: RECENT POLICY AND GUIDANCE ON FEDERAL VULNERABILITY DISCLOSURE PROGRAMS 2–3 (2020) (distinguishing U.S. government's VEP from the VDPs of individual federal agencies). As of March 2021, all U.S. federal agencies, with exceptions for statutorily defined "national security systems" and "certain systems operated by the Department of Defense or the Intelligence Community," are required to have VDPs. OFF. OF MGMT. & BUDGET OFF. OF THE PRESIDENT, OMB MEMO. NO. M-20-32: IMPROVING VULNERABILITY IDENTIFICATION, MANAGEMENT AND REMEDIATION (SEPT. 2, 2020); *Binding Operational Directive BOD 20-01: Develop and Publish a Vulnerability Disclosure Policy*, CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY (Sept. 2, 2020), https://www.cisa.gov/news-events/directives/bod-20-01-develop-and-publish-vulnerability-disclosure-policy [hereinafter *BOD 20-01*). A related policy is CISA's Coordinated Vulnerability Disclosure Process which "coordinates the remediation and public disclosure of newly identified cybersecurity vulnerabilities in products and services" with affected vendors and service providers. The policy includes a five-step process, and its objective is to coordinate simultaneous disclosure of the vulnerability by CISA, affected vendors and service providers, and the vulnerability reporter "to ensure that users and administrators receive clear and actionable information in a timely manner." *Coordinated Vulnerability Disclosure Process*, CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY, https://bit.ly/3STfMyw (last visited Feb. 9, 2024). Notably, the CISA CVD expressly explains its interplay with the U.S. VEP: "While CISA participates in the interagency VEP, vulnerability reports collected by CISA under this policy [CVD] are not subject to adjudication by the VEP participants, per Section 5.4 of the VEP Charter." *Id.*

[30] SEE SOMETHING, SAY SOMETHING, *supra* note 21, at 44.

[31] CEPS, VULNERABILITY DISCLOSURE IN EUROPE, *supra* note 26, at 5.

[32] ALLEN D. HOUSEHOLDER, GARRET WASSERMANN, ART MANION & CHRIS KING, THE CERT® GUIDE TO COORDINATED VULNERABILITY DISCLOSURE 8-11 (Carnegie Mellon University Software Engineering Institute, 2017).

There is a third emerging category of laws relating to vulnerability disclosure that seem to upend the usual criteria and objectives. These laws require companies to notify the government of vulnerabilities that the companies discover in their own systems before they are patched. In July 2021, the People's Republic of China published its "Regulations on the Management of Network Product Security Vulnerabilities" (RMSV), which requires any business operating in China to report vulnerabilities to the Ministry of Industry of Information Technology (MIIT) *before* patching the vulnerability or publicly reporting it.[33] The regulation requires businesses to report software vulnerabilities to the MIIT within forty-eight hours of discovery.[34] Security researchers and some companies have accused China of abusing the RMSV's vulnerability disclosure requirements in an effort to discover and develop zero-day exploits, in effect expanding its vulnerability stockpile.[35] A second example comes from the EU Cyber Resilience Act, proposed in 2022 and currently under debate. The Act's vulnerability disclosure provision would require companies that sell software in Europe to notify the EU standards body within twenty-four hours if the company confirms active exploitation of a previously unknown vulnerability in its systems.[36] Industry leaders have criticized the proposed Act for encouraging government stockpiling practices and incentivizing the abuse of undisclosed vulnerabilities by governments and malicious actors.[37]

---

[33] Cary & Del Rosso*, supra* note 6. The authors explain how the 2021 vulnerability disclosure law is part of a larger effort by China to "collect more vulnerabilities," which includes prohibiting cybersecurity experts from traveling to international security competitions and hosting a series of competitions for the "development of technology that could automate the discovery, exploitation, and patching of software vulnerabilities." *Id.*

[34] Cary & Del Rosso*, supra* note 6 ("In effect, the regulations push all software-vulnerability reports to the MIIT before a patch is available.").

[35] *See, e.g.,* MICROSOFT REPORT 2022, *supra* note 21, at 39 ("The increased use of zero-days over the last year from China-based actors likely reflects the first full year of China's vulnerability disclosure requirements for the Chinese security community and a major step in the use of zero-day exploits as a state priority."); Cary & Del Rosso*, supra* note 6 (finding that "the 2021 RMSV allows the PRC government, and subsequently the Ministry of State Security, to access vulnerabilities previously uncaptured by past regulatory regimes and policies."); Temple-Raston, *supra* note 12 ("I think where we're going with this right now is a dangerous place where governments are starting to propose requirements for companies to disclose vulnerability information for which there are no patches yet. That not only fundamentally breaks the need-to-know basis of vulnerability disclosure, but it actually increases risk all around.").

[36] *EU Cyber Resilience Act*, EUROPEAN COMMISSION (Dec. 1, 2023), https://bit.ly/3SxsIbO.

[37] *Joint Letter of Experts on CRA and Vulnerability Disclosure*, CTR. FOR CYBERSECURITY POL'Y & L., (Oct. 3, 2023), https://bit.ly/3uzcZks; Michael Hill, *Cybersecurity Experts Raise Concerns Over EU Cyber Resilience Act's Vulnerability Disclosure Requirements*, CSO ONLINE (Oct. 3, 2023), https://bit.ly/3UvWZul.

In addition to the vulnerability-related disclosure policies described above, the U.S. government has in place a number of other cyber-related information-sharing policies and authorities. Some of the authorities are statutory and some are found in executive branch directives, some are voluntary and some are mandatory. Regardless of form, their aim is to provide guidance on and channels for industry to share cyber-related information with the U.S. government, and in some instances for the government to share such information with industry.[38]

When was the U.S. VEP established?

The U.S. VEP has its origins in the wake of 9/11 and the growing use of vulnerabilities by governments to accomplish various national security and intelligence objectives.[39] It was tacitly acknowledged by the U.S. government in

[38] For examples of executive orders and presidential directives aimed at encouraging private-sector cyber information-sharing efforts and establishing information-sharing channels with federal government, see Robert Knake, S*haring Classified Cyber Threat Information with the Private Sector*, COUNCIL ON FOREIGN RELS. BLOG (May 15, 2018), https://on.cfr.org/49todFZ [hereinafter Knake, *Sharing*] and *supra* notes 92, 93, 95 and 96 (listing relevant executive orders and directives). For examples of legislative efforts in the information-sharing and notification space, see Cybersecurity Information Sharing Act of 2015, Pub. L. No. 114–113, Div. N, 129 Stat. 2935 (Dec. 18, 2015) (codified at 6 U.S.C. §§ 1501-1510) (incentivizing information sharing between private companies by providing liability protections); Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA), Pub. L No. 117–103, Div. Y, 136 Stat. 1038 (Mar. 15, 2022) (codified at 6 U.S.C. §§ 681–681g) (authorizing CISA to develop and implement regulations requiring covered entities to report covered cyber incidents and ransom payments to CISA); Press Release, U.S. Sec. & Exch. Comm'n, SEC Adopts Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies (July 26, 2023) (requiring registrants to disclose material cybersecurity incidents they experience and adopting rules requiring foreign private issuers to make comparable disclosures). An example of a voluntary public-private cybersecurity collaborative is the Joint Cyber Defense Collaborative (JCDC), established in 2021 and housed in CISA with the goal of "unit[ing] the global cyber community in the collective defense of cyberspace." *JCDC FAQs*, CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY, https://www.cisa.gov/topics/partnerships-and-collaboration/joint-cyber-defense-collaborative/jcdc-faqs (last visited Mar. 12, 2024). The JCDC's participants include service providers, infrastructure operators, cybersecurity companies, companies across the various critical infrastructure sectors, and subject matter experts. *Id.* While the JCDC seeks to provide a model of operational collaboration, its effectiveness has come under criticism "due to a lack of technical expertise and an overabundance of lawyers." Christian Vasquez, *CISA Releases 2024 Priorities for the Joint Cyber Defense Collaborative*, CYBERSCOOP (Feb. 12, 2024), https://cyberscoop.com/cisa-jcdc-2024-priorities/.

[39] For a full accounting of the U.S. VEP's origins and evolution, from HSPD-54 (2008) to the 2010 version (released as part of EFF's FOIA lawsuit) to Michael Daniel's 2014 blog post about the Heartbleed bug to the events leading up to the 2017 publication of the unclassified VEP charter, see Healey, *Zero-Day Vulnerabilities, supra* note 21; Herpig & Schwartz, *supra* note 11; Kim

2014 following the Heartbleed bug in a post by then Special Assistant to the President and Cybersecurity Coordinator Michael Daniel. The acknowledgement of an internal interagency decision-making process was intended to assure industry and the public that the U.S. government took "seriously its commitment to an open and interoperable, secure and reliable Internet," and that the government had "re-invigorated [its] efforts to implement existing policy with respect to disclosing vulnerabilities – so that everyone can have confidence in the integrity of the process we use to make these decisions."[40] Rather than quelling concerns, the post led to significant commentary and calls for additional information as well as recommendations for improvements.[41] In November 2017, arguably in response to the outcry that came in the wake of the WannaCry and NotPetya attacks, the U.S. government published an unclassified charter of the U.S. VEP.[42] The charter identified the key players in the interagency decision-making process, cataloged the equities at issue, outlined the discovery-to-decision timeline, and described the decision-making process when the U.S. government was assessing whether to "disseminate vulnerability information to the vendor/supplier in the expectation that it will be patched, or to temporarily restrict the knowledge of the vulnerability to the USG . . . so that it can be used for national security and law enforcement purposes, such as intelligence collection, military operations, and/or counterintelligence."[43]

Who participates in the U.S. VEP?

The National Security Council (NSC) is charged with coordination of the VEP process, and the charter established an Equities Review Board (ERB) to serve as the primary forum for interagency discussion and determination as to whether to disclose or retain a vulnerability.[44] The review process involves four

Zetter, *U.S. Gov Insists It Doesn't Stockpile Zero-Day Exploits to Hack Enemies*, WIRED (Nov. 17, 2014), https://bit.ly/4997XdE; COUNCIL ON FOREIGN RELS., CONFRONTING REALITY IN CYBERSPACE: FOREIGN POLICY FOR A FRAGMENTED INTERNET 1–40 (2022).

[40] Michael Daniel, *Heartbleed: Understanding When We Disclose Cyber Vulnerabilities,* THE WHITE HOUSE (Apr. 28, 2014), https://bit.ly/48bY7Xb.

[41] *See supra* note 22 and sources cited therein.

[42] U.S. VEP, *supra* note 9; *see also* Press Release, White House Cybersecurity Coordinator Rob Joyce, Improving and Making the Vulnerability Equities Process Transparent is the Right Thing to Do (Nov. 15, 2017) https://trumpwhitehouse.archives.gov/articles/improving-making-vulnerability-equities-process-transparent-right-thing/.

[43] U.S. VEP, *supra* note 9, at Section 1.

[44] *Id.* at Section 2 (explaining "the process is coordinated by the National Security Council (NSC) staff so that multiple agency viewpoints can be considered, informed by the full input and consideration of the interagency experts") & Section 4.1.

types of participants or key players: permanent ERB members, temporary ERB participants, the VEP Director, and the VEP Executive Secretariat.

The **permanent ERB members**[45] include the following departments and agencies, each charged with sending a representative with the authority to represent the views of their agency head:

- Office of Management and Budget
- Office of the Director of National Intelligence (to include Intelligence Community-Security Coordination Center (IC-SCC))
- Department of the Treasury
- Department of State
- Department of Justice (to include the Federal Bureau of Investigation and the National Cyber Investigative Joint Task Force (NCIJTF))
- Department of Homeland Security (to include the National Cybersecurity Communications and Integration Center (NCCIC) and the United States Secret Service (USSS))
- Department of Energy
- Department of Defense (including the National Security Agency (NSA) (including Information Assurance and Signals Intelligence elements)), United States Cyber Command, and DoD Cyber Crime Center (DC3))
- Department of Commerce
- Central Intelligence Agency

Other US Government agencies may engage in the VEP process as **temporary ERB participants**. Such agencies "may participate when demonstrating responsibility for, or identifying equity in, a vulnerability under deliberation."[46] The question, of course, is how these temporary participants know that a vulnerability has been submitted to the VEP for consideration if they are not on the ERB's permanent member list. While far from clear, presumably, notice of submitted vulnerabilities to non-ERB members would occur through the NSC process as laid out in the relevant presidential policy directive.[47]

Each agency participating in vulnerability decisions—whether a permanent ERB member or a temporary ERB participant—must designate a Point of Contact (VEP POC). The VEP POC has three duties: to be responsible for

[45] *Id.* at Section 4.1.
[46] *Id.* at Section 4.1 & Annex A (defining "Equities Review Board (ERB)").
[47] *Id.* at Annex A (referencing NSPM-4 process for coordination of the ERB).

vulnerability submissions for their entity, to serve as the primary contact for any communications from the VEP Executive Secretariat, and to identify a subject matter expert (SME) from their entity as needed to support equities determinations and discussions.[48]

The **VEP Director** is tasked with responsibility for "ensuring effective implementation of VEP policies."[49] The director is housed in the NSC, with the role to be filled by the individual holding the position of "Special Assistant to the President and Cybersecurity Coordinator, or an equivalent successor." The Trump Administration eliminated the Cybersecurity Coordinator position in 2018, so the role now is held by an equivalent successor, presumably the Deputy National Security Advisor for Cyber and Emerging Tech.[50]

The **VEP Executive Secretariat** is held by the National Security Agency, which acts under the authority, direction, and control of the Secretary of Defense.[51] The VEP Director can assign the role to another agency so long as certain conditions are met. To date, there has been no public reporting indicating that the Executive Secretariat has been assigned outside the NSA.[52] The specific duties of the Executive Secretariat are laid out in Section 4.2 and include coordinating information flows and meetings, as well as record keeping.[53] Notably, the charter provides that the "VEP Executive Secretariat will keep formal records of this information to permit later review of the overall efficacy of the process,"[54] although there is no guidance as to who is tasked with conducting that later review. With an understanding of the key players, let's now turn to consider the vulnerability review and determination process.

---

[48] *Id.* at Section 4.1.

[49] *Id.*

[50] At the time of publication, it appears this role is most likely filled by Anne Neuberger who serves as the Deputy National Security Advisor for Cyber and Emerging Tech in the Biden Administration. Although some have suggested the National Cyber Director, a position established by the NDAA for 2021 and first staffed in 2021, now fills the VEP Director role. *See* Polley, *supra* note 22, at 16.

[51] U.S. VEP, *supra* note 9, at Section 4.2.

[52] Under Section 4.2. of the U.S. VEP, the "VEP Director may designate another agency to perform this function with the permission of the head of that agency." *Id. See also infra* Section III.C. (proposing reassignment of the Executive Secretariat).

[53] *Id.* This provision of the charter identifies the following specific duties of the VEP Executive Secretariat: maintain VEP POC, SME, and ERB member contact information; maintain records of all vulnerabilities that have been identified to the VEP Executive Secretariat ("At a minimum, records will include the submitting agency, the dissemination determination and date, and whether reassessment is necessary. Other pertinent information may also be recorded."); create an annual report as described in Section 4.3; and document and maintain records of the contested preliminary determination process described in Section 5.2.6. *Id.*

[54] *Id.*

The first step is to figure out how vulnerabilities are identified and which vulnerabilities are submitted to the review process.

Which vulnerabilities are submitted to the ERB for review?

Well, in practice, not too many. The VEP is limited to considering vulnerabilities that are both "newly discovered"[55] and "not publicly available."[56] As a result of these "threshold"[57] requirements, vulnerabilities that are purchased by the government—rather than developed or discovered by it—are excluded.[58] The purchasing exclusion is in addition to the exceptions laid out in Section 5.4, which exclude from the review process several categories of vulnerabilities: those that are subject to partner agreements with exclusivity clauses or NDA restrictions, which also affects purchased vulnerabilities;[59] those that are part of sensitive operations;[60] those identified through researcher

[55] *Id.* at Annex A (offering definition of "newly discovered" as "After February 16, 2010, the effective date of the initial Vulnerabilities Equities Process, when the USG discovers a zero-day vulnerability or new zero-day vulnerability information, it will be considered newly discovered. This definition does NOT preclude entry of vulnerability information discovered prior to February 16, 2010.").

[56] *Id.* (defining a vulnerability as "publicly known" if "the vendor is aware of its existence and/or vulnerability information can be found in the public domain (e.g., published documentation, Internet, trade journals.").

[57] *Id.* at Section 5.1.

[58] For excellent summaries of the purchasing loophole and the market for cyber-intrusion tools, see Andy Greenberg, *Shopping for Zero-Days: A Price List for Hackers' Secret Software Exploits*, FORBES (Mar. 23, 2012), https://bit.ly/49uFGy4; Andy Greenberg, *Meet the Hackers Who Sell Spies the Tools to Crack Your PC (and Get Paid Six-Figures Fees)*, FORBES (Mar. 21, 2012), https://bit.ly/3w7LVct.; GOOGLE TAG, BUYING SPYING, *supra* note 7; PERLROTH, *supra* note 2, at 39–40.

[59] U.S. VEP, *supra* note 9, at Section 5.4; *see also* Healey, *Zero-Day Vulnerabilities, supra* note 21, at 10 (suggesting there may be a loophole when U.S. uses vulnerabilities provided by allies or other foreign partners).

[60] The term "sensitive operations" is not defined in the VEP. *See* U.S. VEP, *supra* note 9, Section 5.4. Presumably, however, these operations include joint operations with allies or other partners. "[I]f these partners have a vulnerability that they are actively exploiting (or planning to exploit), it is possible that the US Government may need to abide by any disclosure or retention restrictions put in place by these counterparts – even if it goes against an ERB adjudication decision." Polley, *supra* note 22, at 24. Others have pointed out the ability to avoid the ERB review process by labeling any law enforcement or intel operation as "sensitive." Andrew Crocker, *Time Will Tell If the New Vulnerabilities Equities Process Is a Step Forward for Transparency*, EFF BLOG (Nov. 16, 2017), https://www.eff.org/deeplinks/2017/11/time-will-tell-if-new-vulnerabilities-equities-process-step-forward-transparency ("And exempting vulnerabilities involved in 'sensitive operations' seems like an exceptionally wide loophole, since essentially all offensive uses of vulnerabilities are sensitive.").

activity and incident response;[61] and misconfigurations and misuses.[62] Additional information on these exceptions and exemptions is included in Annex C, which is classified. The breadth of the exceptions and exclusions means, in practice, that a number of vulnerabilities never reach the balancing of equities the U.S. VEP is designed to provide.[63] Notably, the unclassified charter does not provide guidance on how agencies should identify vulnerabilities that meet the "threshold" requirements, nor does it identify the consequences for failing to submit vulnerabilities to the review process.

How does the review process work?

Section 5 outlines the review process leading to a restrict-or-disclose determination.[64] An agency will submit a vulnerability that meets the threshold (as described above) to the VEP Executive Secretariat and include with its submission a recommendation as to whether it should be restricted or disseminated.[65] Within one business day, the VEP Executive Secretariat will notify the VEP POCs for each of the ERB member agencies of the vulnerability and ask them to respond if they have an equity at stake. If an agency claims an equity, it has five days to indicate whether it concurs with the recommendation of the submitting agency. If the agency claiming an equity disagrees with the recommendation of the submitted agency they are considered to be "non-concurring." The next step involves a meeting between the submitting agency, the non-concurring agency or agencies, and the VEP Executive Secretariat with the goal of reaching consensus on whether to restrict or disclose. If this initial group cannot reach consensus, they will prepare options for consideration by the full ERB. If the ERB members cannot reach consensus, which is the charter's preferred path, then they will vote to come up with a "preliminary determination" as to whether to restrict or disclose. If no agency contests the preliminary determination within five days, it will be

---

[61] U.S. VEP, *supra* note 9, at Section 5.4.

[62] *Id.*

[63] *See infra* Section II.C.3 (describing lingering concern about U.S. VEP's exclusions and exceptions).

[64] U.S. VEP, *supra* note 9, at Section 5.

[65] *Id.* at Section 5.2. A later section of the VEP provides more detailed guidance when the vulnerability is discovered in a certain type of equipment or platform. If a vulnerability is "found in GOTS equipment or systems that were certified by NSA, or in any cryptographic function, whether in hardware or software, certified or approved by NSA, then the vulnerability will be reported to NSA as soon as practical." *Id.* at Section 5.3. In such instances, the NSA "will assume responsibility for this vulnerability and submit it formally through the VEP Executive Secretariat." *Id.*

treated as final and implemented. If, however, an agency with an equity disputes the preliminary determination, they must provide notice to the VEP Executive Secretariat within five days of the preliminary determination, and the VEP Executive Secretariat then notifies the VEP Director. The dispute then moves to the NSC—or similar interagency meeting venue—and follows the resolution process laid out in the relevant national security memorandum.[66]

What equities are considered during the review?

The term "equities" captures the idea that the use or exposure of a single vulnerability creates the potential for significant conflict between competing interests. "Governments will need to weigh how to protect the public, critical infrastructure and even government services online from attacks and breaches—but also how to ensure that one agency is not accidentally interfering with the work of another."[67] These competing interests exist within the government between various agencies and departments, with different agencies seeking to exploit and protect against the same vulnerability. The competing interests also exist between the government and external entities; these include the interests of industry, commerce, critical infrastructure protection, international relationships, privacy, and civil liberty.[68] The U.S. VEP's purpose, of course, is to balance such equities and to do so in a manner that "prioritize[s] the public's interest in cybersecurity and [] protect[s] core Internet infrastructure, information systems, critical infrastructure systems, and the U.S. economy through the disclosure of vulnerabilities discovered by the USG, absent a demonstrable, overriding interest in the use of the vulnerability."[69] Annex B identifies four categories of equities to be considered in the process: defensive; intelligence, law enforcement and operational; commercial; and international partnerships.[70]

---

[66] *See* U.S. VEP, *supra* note 9, at Section 5.2.6, Figure 1 in Section 5.2 (providing a workflow chart and referencing NSPM-4 (Trump Administration), which now has been replaced by NSM-2 (Biden Administration)).

[67] Herpig & Schwartz, *supra* note 11.

[68] U.S. VEP, *supra* note 9, Section 5.2.4 (explaining that retain-disclose decisions will be made in "overall best interest of USG missions of cybersecurity, intelligence, counterintelligence, law enforcement, military operations, and critical infrastructure protection"); MORE SUNLIGHT, *supra* note 11, at 4 (describing national interests in "CI protection, citizens' privacy and civil liberties, and trust in government within and across countries" and a government's need to use vulnerabilities "to achieve important law enforcement, public safety, and national security goals").

[69] U.S. VEP, *supra* note 9, Section 1.

[70] *Id.* at Annex B.

Defensive:

1.A. Threat Considerations

- Where is the product used? How widely is it used?
- How broad is the range of products or versions affected?
- Are threat actors likely to exploit this vulnerability, if it were known to them?

1.B. Vulnerability Considerations

- What access must a threat actor possess to exploit this vulnerability?
- Is exploitation of this vulnerability alone sufficient to cause harm?
- How likely is it that threat actors will discover or acquire knowledge of this vulnerability?

1.C. Impact Considerations

- How much do users rely on the security of the product?
- How severe is the vulnerability? What are the potential consequences of exploitation of this vulnerability?
- What access or benefit does a threat actor gain by exploiting this vulnerability?
- What is the likelihood that adversaries will reverse engineer a patch, discover the vulnerability and use it against unpatched systems?
- Will enough USG information systems, U.S. businesses and/or consumers actually install the patch to offset the harm to security caused by educating attackers about the vulnerability?

I.D. Mitigation Considerations

- Can the product be configured to mitigate this vulnerability? Do other mechanisms exist to mitigate the risks from this vulnerability?
- Are impacts of this vulnerability mitigated by existing best-practice guidance, standard configurations, or security practices?
- If the vulnerability is disclosed, how likely is it that the vendor or another entity will develop and release a patch or update that effectively mitigates it?
- If a patch or update is released, how likely is it to be applied to vulnerable systems? How soon? What percentage of vulnerable systems will remain forever unpatched or unpatched for more than a year after the patch is released?

- Can exploitation of this vulnerability by threat actors be detected by USG or other members of the defensive community?

Operational:

2.A. Operational Value Considerations

- Can this vulnerability be exploited to support intelligence collection, cyber operations, or law enforcement evidence collection?
- What is the demonstrated value of this vulnerability for intelligence collection, cyber operations, and/or law enforcement evidence collection?
- What is its potential (future) value?
- What is the operational effectiveness of this vulnerability?

2.B. Operational Impact Considerations

- Does exploitation of this vulnerability provide specialized operational value against cyber threat actors or their operations? Against high-priority National Intelligence Priorities Framework (NIPF) or military targets? For protection of warfighters or civilians?
- Do alternative means exist to realize the operational benefits of exploiting this vulnerability?
- Would disclosing this vulnerability reveal any intelligence sources or methods?

Commercial:

- If USG knowledge of this vulnerability were to be revealed, what risks could that pose for USG relationships with industry?

International:

- If USG knowledge of this vulnerability were to be revealed, what risks could that pose for USG international relations?

While the ERB is not limited to only the considerations in Annex B, the list is designed to represent general concerns in the retain-disclose space and to capture the "public's interest" through the review process.[71] Notably, the quantity of disclosure-leaning equities (identifying industry, privacy, and civil liberty interests, among others) appear to be outweighed by the quantity of

[71] U.S. VEP, *supra* note 9, at Annex B ("Evaluations will not be limited to applying only these considerations, but these represent general concerns, which should apply to all vulnerability equity decisions.").

retention-learning equities (those identifying national security, law enforcement, and intelligence interests).

What determination options does the ERB have?[72]

Although we often refer to the U.S. VEP as setting up a "retain or disclose" —or "restrict or disseminate" —process, the determination is not a binary one. Rather, at the conclusion of the equities balancing process, the ERB will consider a spectrum of options between full disclosure and absolute restriction of any knowledge of the vulnerability. These middle-ground options include: disseminating mitigation information to certain entities without disclosing the particular vulnerability; restricting disclosure but limiting the U.S. government's use of the vulnerability in certain ways; informing U.S. government entities and allied government entities of the vulnerability at the classified level; or, using "indirect means" to inform the vendor of the vulnerability.[73] Regardless of the option selected, it should be informed by an "understanding of risks of dissemination, the potential benefits of government use of the vulnerabilities, and the risks and benefits of all options in between."[74]

What happens once the ERB makes a determination?

ERB determinations are supposed to happen "quickly" and in a "timely fashion."[75] The final determination should include a set of agreed-upon guidelines for the use of the vulnerability and guidance on the need for follow-on actions or further review. The "disseminate or restrict" determination is not the end of the process; it is "only one element of the vulnerability equities evaluation process."[76] A determination to "restrict"—or keep secret the vulnerability—is reassessed by the ERB on an annual basis until one of three outcomes occurs: "dissemination is accomplished, the vulnerability is publicly known, or the vulnerability is otherwise mitigated."[77] In addition, should an entity of the U.S. government learn that a retained vulnerability has come into the hands of a malicious actor, that entity must immediately notify the VEP

[72] *See infra* Section II.C (describing representation problems with current U.S. VEP).
[73] *Id.* at Section 1.
[74] *Id.* at Section 1
[75] *Id.* at Section 5.2.4.
[76] *Id.* at Section 1.
[77] *Id.* at Section 5.2.5.

Executive Secretariat, and within one business day of notification, the ERB must meet to decide what further action to take.[78]

Does the U.S. VEP include any oversight provisions?

In a subtle nod to the concept of oversight, Section 4.3 requires the production of an annual report, prepared and produced by the VEP Executive Secretariat.[79] The report must be submitted to the VEP POCs and the NSC staff. The report should be written at the lowest classification level permissible and should include an executive summary at an unclassified level. The contents of the report should include "statistical data as deemed appropriate by the VEP Director" and then any changes to the ERB membership, a reassignment of the VEP Director position, or realignment of the VEP Executive Secretariat's responsibility from the NSA to another agency.[80] Notably, the annual report *may* also be submitted to Congress, although the charter does not require congressional reporting, nor does it specify a particular committee or recipient of the report.[81]

Do other countries have policies like the U.S. VEP?

Yes, but only a handful of governments beyond the U.S. have published either government disclosure decision processes or equity-based vulnerability review processes.[82] Following the publication of the U.S. VEP in 2017, the U.K. published its Equities Process in 2018, followed in 2019 by Australia's Responsible Release Principles for Cyber Security Vulnerabilities, and Canada's Equities Management Framework.[83] In addition, a small number of countries

[78] *Id.* at Section 5.3.
[79] *Id.* at Section 4.3.
[80] *Id.*
[81] *Id. See infra* Section II.C.5 (describing lack of effective accountability mechanisms).
[82] *See supra* notes 24–32 and accompanying text (describing various vulnerability disclosure policies).
[83] Ian Levy, *Equities Process: Publication of the UK's Process for How We Handle Vulnerabilities*, NAT'L CYBER SECURITY CENTRE (Nov. 29. 2018), https://bit.ly/3w8vsVI; Gov't of Australia, AUSTRALIAN SIGNALS DIRECTORATE, RESPONSIBLE RELEASE PRINCIPLES FOR CYBER SECURITY VULNERABILITIES (2019), https://www.asd.gov.au/about/accountability-governance/publications/information-security/responsible-release-principles-cyber-security-vulnerabilities; GOV'T OF CANANDA, COMMUNICATIONS SECURITY ESTABLISHMENT'S (CSE) EQUITIES MANAGEMENT FRAMEWORK (May 11, 2022), https://www.cse-cst.gc.ca/en/information-and-resources/announcements/cses-equities-management-framework.

are on the "path to developing" publicly available VEP or GDDP policies, including Germany, Japan, and Lithuania.[84]

Has the U.S. VEP been updated since 2017 or impacted by more recent executive, legislative, or international law developments?

While the U.S. government has not publicly released a new VEP, there may be an entirely new internal policy governing vulnerabilities which is classified and has not yet made its way into the public eye. There have been, however, several developments on the domestic front and international stage that may implicate how the U.S. VEP is working in practice, whether in its 2017 form or a new and revised edition.

Since the publication of the U.S. VEP in 2017, a swath of executive branch directives and policies have been issued regarding the government's defensive responsibilities relating to cybersecurity as well as the government's offensive use of cyber capabilities to accomplish national security, intelligence, and law enforcement objectives. These include most notably the following authorities listed in reverse chronological order: Executive Order 14117 on Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern (Feb. 2024)[85]; Executive Order 14105 on Addressing United States Investments in Certain National Security Technologies and Products in Countries of Concern (Aug. 2023)[86]; National Cybersecurity Implementation Plan (July 2023)[87]; 2023 National Cybersecurity Strategy (Mar. 2023)[88] which replaced the 2018 National Cyber Strategy; Department of Defense Cyber Strategy (May 2023)[89] which replaced the 2018 DoD Cyber Strategy; Executive Order 14093 on Prohibition on the Use by the United States Government of Commercial Spyware That Poses

---

[84] Polley, *supra* note 22, at 41–42; *see also* Herpig & Schwartz, *supra* note 11 (examining United Kingdom's publication of vulnerability equity balancing policy and Germany's movement toward such a policy).

[85] Exec. Order No. 14,117, Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern, 89 Fed. Reg. 15421 (Feb. 28, 2024) (to be codified at 27 C.F.R. pt. 202).

[86] Exec. Order No. 14,105, Addressing United States Investments in Certain National Security Technologies and Products in Countries of Concern, 88 Fed. Reg. 54867 (Aug. 9, 2023).

[87] WHITE HOUSE, NATIONAL CYBERSECURITY IMPLEMENTATION PLAN (2023).

[88] WHITE HOUSE, NATIONAL CYBERSECURITY STRATEGY (2023) [hereinafter NAT'L CYBERSECURITY STRATEGY].

[89] DEP'T OF DEF., NATIONAL CYBER STRATEGY (2023).

Risks to National Security (Mar. 2023)[90]; Executive Order 14086 on Enhancing Safeguards for United States Signals Intelligence Activities (Oct. 2022)[91]; and Executive Order 14028 on Improving the Nation's Cybersecurity (May 2021).[92]

The U.S. VEP also dances with a number of other executive branch authorities in the legal architecture governing the use of vulnerabilities, some of which predate the publication of the November 2017 Charter. These include Presidential Policy Directive/PPD-41: United States Cyber Incident Coordination (July 2016)[93]; the Biden administration successor to National Security Presidential Memorandum/NSPM-13 (Aug. 2018)[94]; Executive Order 13636 on Improving Critical Infrastructure Cybersecurity (Feb. 2013)[95]; and

[90] Exec. Order No. 14,093, Prohibition on Use by the United States Government of Commercial Spyware that Poses Risks to National Security, 88 Fed. Reg. 18957 (Mar. 27, 2023). "The United States has fundamental national security and foreign policy interests in (1) ensuring that technology is developed, deployed, and governed in accordance with universal human rights; the rule of law; and appropriate legal authorization, safeguards, and oversight, such that it supports, and does not undermine, democracy, civil rights and civil liberties, and public safety; and (2) mitigating, to the greatest extent possible, the risk emerging technologies may pose to United States Government institutions, personnel, information, and information systems." *Id.*

[91] Exec. Order No. 14,086, Enhancing Safeguards for United States Signals Intelligence Activities, 87 Fed. Reg. 62283 (Oct. 7, 2022). This order was aimed at working toward the commitments of the EU-US Data Privacy Framework and UK-US Data Bridge Extension, and included a mandate to establish the Data Protection Review Court. Although the review court does not have express jurisdiction over vulnerabilities, the ability to review and issue remedies relating to governmental signals intelligence and surveillance practices indicate a lean toward more robust oversight. The player here is the judiciary which traditionally has been excluded from oversight of cyber-related activities due to the political question, standing, and/or state secrets doctrines. *See* Data Protection Review Court, 87 Fed. Reg. 62303 (Oct. 14, 2022) (to be codified at 15 C.F.R. pt. 30).

[92] Exec. Order No. 14,028, Improving the Nation's Cybersecurity, 86 Fed. Reg. 26633 (May 12, 2021).

[93] *Presidential Policy Directive/PPD-41: United States Cyber Incident Coordination*, THE WHITE HOUSE (July 26, 2016), https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident.

[94] National Security Presidential Memorandum/NSPM-13 (Aug. 2018) (classified presidential directive available at Presidential Directives & Executive Orders, Federation of American Scientists, https://perma.cc/FD8N-29HQ). *See also* Amy C. Gaudion, *Answering the Cyber Oversight Call*, 54 LOYOLA U. CHI. L.J. 139, 152–53 (2022) (citations omitted) [hereinafter Gaudion, *Answering*] (acknowledging classified nature of such directives, summarizing implications of shift from extensive interagency process outlined in PPD-20 (Obama Administration) to streamlined process adopted in NSPM 13 (Trump Administration), and considering likely policy updates in the Biden Administration).

[95] Exec. Order No. 13,636, Improving Critical Infrastructure Cybersecurity, 78 Fed. Reg. 11739 (Feb. 12, 2013).

Presidential Policy Directive/PPD-21: Critical Infrastructure Security and Resilience (Feb. 2013)[96].

On the legislative side, several developments are noteworthy. The first is the express authorization for offensive cyber operations—which often are accomplished by the use of zero-day vulnerabilities and other cyber-intrusion capabilities—granted in the National Defense Authorization Act for Fiscal Year 2019.[97] Second, the National Defense Authorization Act for Fiscal Year 2023 included several provisions relating to foreign commercial spyware vendors, tasking the Director of National Intelligence (DNI) with gathering information on foreign commercial spyware vendors,[98] and granting the DNI the authority to "prohibit any element of the intelligence community from procuring, leasing, or otherwise acquiring on the commercial market, or extending or renewing a contract to procure, lease, or otherwise acquire, foreign commercial spyware."[99] Finally, the National Defense Authorization Act for Fiscal Year 2024 included a mandate that the Department of State engage in cyber diplomacy by developing bilateral partnerships as well as a mandate to the Department's Bureau of Cyberspace and Diplomacy "to increase secure internet access and digital infrastructure in emerging markets."[100] Two recent legislative actions also are worth noting although their viability is unclear. On March 13, 2024, the U.S. House of Representatives passed a bill that would ban TikTok in the U.S. unless it was divested of its foreign (Chinese) ownership,

---

[96] *Presidential Policy Directive/PPD-21: Critical Infrastructure Security and Resilience*, THE WHITE HOUSE (Feb. 12, 2013), https://obamawhitehouse.archives.gov/the-press-office/2013/02 /12/preside ntial-polic y-directive-critical-infrastructure-security-and-resil.

[97] John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115–232, § 1636, 132 Stat. 2123–24 (2018); *see also* Gaudion, *Answering, supra* note 94, at 149–52 (describing burgeoning statutory authorities for military cyber operations).

[98] National Defense Authorization Act for Fiscal Year 2023, Pub. L. No. 117–263, § 6318, 1136 Stat. 2395 (2022) [hereinafter NDAA FY23]. These include "a report with an accompanying classified annex containing an assessment of the counterintelligence threats and other risks to the national security of the United States posed by the proliferation of foreign commercial spyware" (prepared by the DNI with input from CIA, FBI and NSA—all potential purchasers of vulnerabilities from such companies) and an accompanying classified annex, prepared by the DNI, that provides "a watchlist of companies selling, leasing, or otherwise providing foreign commercial spyware that the Director determines are engaged in activities that pose a counterintelligence risk to personnel of the intelligence community." *Id.* § 6318, 1136 Stat. at 3517. For a discussion of how these requirements and authorities fit in the wider regulatory scheme for commercial spyware, see Lubin, *supra* note 12, at 8–9.

[99] NDAA FY23, § 6318, 1136 Stat.. at 3517. The act also includes considerations to be taken into account when the DNI exercises the authority, *id.* at 3518.

[100] Jonathan G. Cedarbaum & Matt Gluck, *iCyber Provisions in the FY 2024 NDAA*, LAWFARE (Jan. 22, 2024), https://bit.ly/48aO9Fm (describing National Defense Authorization Act for Fiscal Year 2024, Pub. L. No. 118-31, 137 Stat. 136 (2023)).

and a week later the House passed a bill that would ban data brokers from transferring, selling or providing access to certain sensitive personal data of Americans to foreign adversaries.[101] At the time of publication, both bills are pending in the U.S. Senate.

While none of the executive or legislative branch developments noted above expressly mention the U.S. VEP, they are noteworthy for their attempts to work around, alongside, and supplemental to the government's use of vulnerabilities and other cyber-intrusion technologies. They seem to carve out space for the relevant government agencies to continue using vulnerabilities in support of law enforcement, intelligence collection, and other national security objectives.

Let's shift now to highlight how recent developments on the international stage may impact the use of vulnerabilities by the U.S. government. First, as noted above, are the efforts by some governments, China and the EU, to mandate the reporting of vulnerability information by companies to the government prior to patching.[102] Such laws may lead to larger vulnerability stockpiles and increased risk as they "widen the circle of potential exploitation" and upend the ISO standards and "need-to-know" pre-patch norms.[103] Pulling in the other direction are two developments that indicate increasing concern with the use of vulnerabilities by government and the desire for express prohibitions and more stringent oversight mechanisms. These include the Pall Mall Process,[104] which was convened in February 2024, and the Third Summit on Democracy[105] held in March 2024. Both initiatives are likely to impact how

---

[101] Protecting Americans from Foreign Adversary Controlled Applications Act, H.R. 7521, 118th Cong. (2024); Protecting Americans' Data from Foreign Adversaries Act of 2024, H.R. 7520, 118th Cong. (2024).

[102] *See supra* notes 33–37 and accompanying text (describing China's Regulations on the Management of Network Product Security Vulnerabilities (RMSV) and the EU's proposed Cybersecurity Resilience Act).

[103] Temple-Raston, *supra* note 12.

[104] The Pall Mall Process on "Tackling the Proliferation and Irresponsible Use of Commercial Cyber Intrusion Capabilities" gathered participant representatives of states, international organizations, private industry, academia, and civil society to participate in an international conference hosted by the United Kingdom and France. The initiative's aim is to "establish guiding principles and highlight policy options for States, industry and civil society in relation to the development, facilitation, purchase, and use of commercially available cyber intrusion capabilities." *See Pall Mall Process, supra* note 7.

[105] The first Summit for Democracy was held in December 2021 with the aim to bring "together government, civil society and private sector leaders to form a global agenda for democratic renewal." Summit for Democracy, https://summitfordemocracyresources.eu/about/about-the-summit-for-democracy/. One of the outgrowths of the first summit was the establishment of the Export Controls and Human Rights Initiative, "a multilateral effort intended to counter state

the U.S. thinks about its governing structures for the use of vulnerabilities and other cyber-intrusion related capabilities.[106]

From these developments, several takeaways may be discerned. First, the 2023 strategy documents indicate a shift by the U.S. government toward increased regulatory muscle which may impact public-private information-sharing and operational collaboration about vulnerabilities. Second, the recent legislative and executive branch attention on commercial spyware aligns with many of the critiques surrounding the U.S. VEP and may be a harbinger of calls for significant reform. Put bluntly, commercial spyware vendors are the primary sellers of zero-day vulnerabilities to governments, so limits on the ability of U.S. government agencies to engage with *foreign* commercial spyware

---

and non-state actors' misuse of goods and technology that violate human rights." *Export Controls and Human Rights Initiative Code of Conduct Released at the Summit for Democracy*, U.S. DEP'T OF STATE (Mar. 30, 2023), https://www.sta te.gov/export-controls-and-human-rights-initiative-code-of-conduct-released-at-the-summit-fo r-democracy/. The second summit, held in March 2023, saw continued focus on governmental use of commercial cyber-intrusion and spyware tools, with the issuance of Executive Order 14093 on Prohibition on the Use by the United States Government of Commercial Spyware That Poses Risks to National Security (Mar. 27, 2023), the Guiding Principles on Government Use of Surveillance Technologies, and the voluntary Code of Conduct for Enhancing Export Controls of Goods and Technology That Could be Misused and Lead to Serious Violations or Abuses of Human Rights. *Id.* The third summit, hosted by the Republic of Korea, will be held in March 2024 and commentators anticipate additional international discussion of the use of cyber-related tools by democratic governments. A March 2024 press release announcing sanctions against Intellexa Consortium members and entities for commercial spyware violations highlighted the connection, noting that "[i]n advance of the third Summit for Democracy, this action supports the Biden-Harris Administration's government-wide effort to counter the risks posed by commercial spyware and to establish robust protections against the misuse of such tools." U.S. Dep't of Treasury, Press Release: Treasury Sanctions Members of the Intellexa Commercial Spyware Consortium (Mar. 5, 2024), https://home.treasury.gov/news/press-releases/jy2155#:~:text=In%20advance%20of%20the%20third,the%20misuse%20of%20such%20tools.

[106] In addition to the international developments mentioned in the preceding notes, the recent UN effort to draft a cybercrime treaty may alter how governments use vulnerabilities. *See* Tomaso Falchetta, *The Draft UN Cybercrime Treaty Is Overbroad and Falls Short on Human Rights Protection*, JUST SEC. (Jan. 22, 2024), https://bit.ly/3uruwv4 (describing January 2024 debates on draft UN cybercrime treaty). For example, "the provision detailing the powers of search and seizure of information stored in a digital device (paragraph 4 of Article 28) is worded in a way that may result in States imposing obligations upon telecommunications and internet service providers to either disclose vulnerabilities of certain software or to provide relevant authorities with access to encrypted communications. This would open the door to government hacking or even undermine or weaken encryption, thereby compromising the privacy and security of digital communications." *Id.* For a fuller examination of international developments relating to governmental use of cyber-intrusion capabilities, see Lubin, *supra* note 12, at 13–17 (summarizing efforts by international actors including the Wassenaar Arrangement, Export Controls and Human Rights Initiative, and recently adopted "Code of Conduct for Enhancing Export Controls of Goods and Technology That Could be Misused and Lead to Serious Violations or Abuses of Human Rights").

vendors may lessen the flow of zero-days coming in. Third, the legislative mandates to the U.S. State Department to engage in cyber diplomacy and to prioritize secure internet access and digital infrastructure may come crashing up against other equities in the ERB review process or at least cause a recalibration of the weights in the restrict-disseminate determination step. Fourth, the establishment of the Cyber Safety Review Board and the State Department Bureau of Cyberspace and Digital Policy may indicate larger roles for private sector and foreign partners in vulnerability-related decisions. Fifth, and finally, trends on the international stage also may impact future iterations of the U.S. VEP and the government's use of vulnerability-enabled tools and capabilities.

Was EternalBlue subject to an equities review process?

Maybe. Having established a general understanding of vulnerability equity weighing and disclosures processes and a primer on the U.S VEP, let's turn now to consider how a VEP-like review process might work in practice. Consider the zero-day vulnerability that the U.S. government used to develop its EternalBlue exploit, and let's re-create what the U.S. government's decision-making process might have looked like, using a series of questions organized loosely by the process stages:

Submission	• Was the EternalBlue vulnerability submitted to the ERB? • Did it meet the threshold requirements of being "newly discovered" and "not publicly known"? • Or was it purchased or subject to one of the other exclusions or exceptions (in which case it was not subject to the ERB review process)? • Which U.S. agency discovered the vulnerability?
Notification	• Did the VEP Executive Secretariat send notice of the EternalBlue vulnerability only to ERB Permanent Members? Or did it send notice to any other federal agencies? • Did any non-ERB member agencies demonstrate responsibility for or identify an equity in the EternalBlue vulnerability?

Equity Considerations	• What was the submitting agency's initial "disseminate or restrict" recommendation for the EternalBlue vulnerability? • Was there consensus agreement with the submitting agency's initial recommendation or did any agency claim an equity or issue a non-concur? • What equities were considered? • How was the demonstrated operational value of the vulnerability measured? • What high-priority targets would the vulnerability allow operations against? • Were there any alternative means to realize the same operational benefits that EternalBlue would provide? • How significant were the concerns that other threat actors (like the Shadow Brokers) would discover or acquire knowledge of the vulnerability? • How did the government measure the potential economic impact on U.S. businesses and/or consumers? On international businesses and/or consumers? • How did the government measure the likelihood that U.S. businesses and/or consumers would install a patch if the vulnerability was disclosed? • Which agencies represented Microsoft's perspective during the discussion? • What risks to U.S. industry and risk to the government's relationship with U.S. industry did the government consider? • What risks to the government's international relationship did the government consider? • If the vulnerability went to the ERB determination process, was there consensus among the ERB or did the issue go to a preliminary determination vote? • Did any agency challenge or dispute the preliminary determination?

Determination	• Once the determination was made, did the ERB put in place any mitigating measures? • Did it share the vulnerability with foreign partners? • Did it restrict use of the vulnerability to certain types of offensive operations?
Follow-On Actions	• How often, during the five years of retention of the EternalBlue vulnerability, was the initial determination reassessed or reviewed? • What additional equities were considered in the reassessments? • Did the VEP Executive Secretariat invite any agencies to the reassessments that were not involved in the initial review of EternalBlue? • Did the reassessments result in any mitigating measures?

And there is one final question to consider: If the vulnerability had not been leaked, would the U.S. government have continued to retain and use it?

In retroactively role-playing how the U.S. government reached its decision not to disclose the vulnerability that led to WannaCry and NotPetya, we can more fully understand the equities at stake in VEP decisions while appreciating the consequences and tradeoffs of a retention decision. While there is little doubt that vulnerability-enabled operations are essential to national defense and law enforcement, the WannaCry and NotPetya attacks revealed important lessons regarding the "friendly fire" potential for unintended and far-reaching effects and the need for post-decision review, transparency, and vigorous oversight. The question then becomes identifying the entity best equipped to provide the appropriate level of oversight.

II. A VIEW FROM THE CAPITOL: VULNERABILITIES AND CONGRESS

The use of vulnerabilities is premised on the idea that the intelligence gain or security advantage is so high that it outweighs the interest in a secure and accessible internet and the privacy of individual consumers. The overarching goal of any equities balancing process is to strike the balance between the competing interests appropriately. On paper, the U.S. VEP appears to be

achieving that goal. In practice, however, concerns linger. This section describes the existing oversight authorities that guide the government's disclosure of vulnerabilities. This part examines recent congressional efforts to gain information about the executive branch's VEP. It focuses on the initial codification efforts in 2017 following the Shadow Brokers leak and the WannaCry and NotPetya incidents. It then shifts attention to reporting requirements in the National Defense Authorization Act for Fiscal Year 2020, and embedded Intelligence Authorization Acts for Fiscal Years 2018, 2019, and 2020, as well as subsequent attempts to mold the U.S. VEP through other disclosure-related policies. This part concludes by cataloging lingering concerns about the poor fit between the government activity in need of oversight—its use of vulnerabilities for offensive operations—and the institutions tasked with providing that oversight.

A. Early Codification Attempts

The most notable legislative efforts came in the spring of 2017 as the WannaCry and NotPetya attacks wreaked havoc, and news stories revealed the exploit had its origins in the NSA. Identical versions of the Protecting Our Ability to Counter Hacking Act (PATCH Act) were introduced in May 2017 in both the U.S. House and Senate.[107] Several aspects of the bills are noteworthy for our purposes. At the most basic level, they sought to codify the U.S. VEP's review and balancing process, with a few redesign tweaks. In contrast to the executive branch policy in place at the time, the bills situated the chair of the review board in the Department of Homeland Security (not the NSA), required all federal agencies to submit information (not only those listed), expanded the committees who would receive reports on the U.S. VEP's review process (beyond the intelligence committees to include the committees on commerce, energy and homeland security), and carved out express roles for internal oversight entities (requiring a report from the Inspector General of the Department of Homeland Security and providing for review and consultation with the Privacy and Civil Liberties Oversight Board (PCLOB)).[108] While

[107] Protecting our Ability To Counter Hacking (PATCH) Act of 2017, H.R. 2481, 115th Cong. (2017); Protecting our Ability To Counter Hacking (PATCH) Act of 2017, S. 1157, 115th Cong. (2017); *see also* Mailyn Fidler & Trey Herr, *PATCH: Debate Codification of the VEP*, LAWFARE (May 17, 2017), https://bit.ly/49rUmxD (evaluating bills and considering benefits and concerns of codifying the equities balancing process).

[108] *See, e.g.*, H.R. 2481 Section 2(c)(1)(A) ("The Secretary of Homeland Security, or the designee of the Secretary, who shall be the chair of the Board."); Section 2(d)(2) ("The head of each

neither bill made it out of committee, they reflected congressional attention and may have contributed to the White House's release of the revamped policy six months later in November 2017. After additional efforts at codification of the U.S. VEP failed,[109] the congressional tool of choice became reporting requirements.

B. Congressional Reporting—The Next Best Thing?

After several earlier attempts stalled, Congress passed statutory reporting requirements for the U.S. VEP in Section 6720 of the National Defense Authorization Act for Fiscal Year 2020, codified at 50 U.S.C. § 3316a.[110] The first of the three mandates required the Director of National Intelligence to submit, by approximately March 20, 2020, an initial written report to the Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence that described for each element of the intelligence community, the "title of the official or officials responsible for determining whether, pursuant to criteria contained in the Vulnerabilities Equities Policy and Process document or any successor document, a vulnerability must be submitted for review under the Vulnerabilities Equities Process" and the "the process used by such element to make such determination."[111] In addition, the report should describe the "roles or responsibilities of that element during a review of a vulnerability submitted to the Vulnerabilities Equities Process."[112] The report should be submitted in unclassified form, but could include a classified appendix.[113] Take note that this report seeks information about only some of

---

Federal agency shall, upon obtaining information about a vulnerability that is not publicly known, subject such information to the process"); Section 2(f)(2) ("[T]he Inspector General of the Department of Homeland Security shall, in consultation with the Inspectors General of other Federal agencies whose work is affected by activities of the Board, submit to the appropriate committees of Congress a report on the activities of all such Inspectors General during the preceding year in connection with the activities of the Board"); Section 2(f)(4) ("The Privacy and Civil Liberties Oversight Board shall review each report"); Section 2(f)(5) (identifying committees).

[109] *See id.* For a full summary of these legislative efforts, see Polley, *supra* note 22, at 35–37.

[110] National Defense Authorization Act for Fiscal Year 2020, Pub. L. No. 116-92, § 6720, 133 Stat. 2230 (2019) ("Reports of Intelligence Community Participation in Vulnerabilities Equities Process of Federal Government"). From a legislative tracking perspective, it bears noting that the Intelligence Authorizations Acts for Fiscal Years 2018, 2019 and 2020 were included in the NDAA for FY 2020, Pub. L. No. 116-92, § 2, 133 Stat. 1198, 1198 (2019) (noting inclusion of IAAs in the Table of Contents).

[111] 50 U.S.C. § 3316a(b)(1(A).

[112] *Id.* at § 3316a(b)(1)(B).

[113] *Id.* at § 3316a(b)(3).

the players in the VEP process—those players that are "elements of the intelligence community."

The second reporting mandate also limited its reach to elements of the intelligence community. If any such element made a "significant change" in its process or criteria for determining whether to submit a vulnerability to the U.S. VEP, that element was required to submit a report to the congressional intelligence committees describing that change within thirty days of the change being made.[114]

The third reporting requirement mandated that the DNI provide an annual classified report to the congressional intelligence committees that described: the number of vulnerabilities submitted for VEP review; of the number submitted for review, the number of vulnerabilities disclosed to each vendor responsible for correcting the vulnerability, or to the public; and the aggregate number, by category, of the vulnerabilities excluded from review under the Section 5.4 of the Vulnerabilities Equities Policy and Process document.[115] In addition, the annual report should include an "unclassified annex" that contained the "the aggregate number of vulnerabilities disclosed to vendors or the public" and "the aggregate number of vulnerabilities disclosed to vendors or the public . . . known to have been patched."[116] A few years later, Congress returned to the oversight task and added a requirement that the DNI "make available to the public each unclassified appendix" submitted with an annual report.[117]

Notably, the Act's "nonduplication" provision allows the DNI to forgo submission of the annual report if the Director "notifies the intelligence committees in writing that . . . an annual report required by paragraph 4.3 of the [VEP] already has been submitted to Congress, and such annual report contains the information that would otherwise be required to be included in an annual report under this subsection."[118]

Similar to the earlier failed attempts at codification, earlier drafts of the bills that ultimately led to the statutory reporting requirements had carved out an express role for an internal oversight entity. In the earlier House and Senate versions of the IAA for FY2018, the Inspector General of the Intelligence

---

[114] *Id.* at § 3316a(b)(2).
[115] *Id.* at § 3316a(c)(1).
[116] *Id.* at § 3316a(c)(2).
[117] *Id.* at § 3316a(c)(4). *See* Pub. Law. 117–103 (Consolidated Appropriations Acts of 2022), which amended 50 U.S.C. 3316a(c) by adding at the end the following: "(4) PUBLICATION. —The Director of National Intelligence shall make available to the public each unclassified appendix submitted with a report under paragraph (1) pursuant to paragraph (2).").
[118] 50 U.S.C. § 3316a(c)(3).

Community would have been tasked with conducting a review and issuing a report on "the roles and responsibilities of the elements of the intelligence community in the process of the Federal Government for determining whether, when, how, and to whom information about a vulnerability that is not publicly known will be shared with or released to a non-Federal entity or the public."[119] While the assignment of the U.S. VEP oversight role to this particular player did not survive the legislative process, it is a proposal that bears further study and consideration.[120]

C. Lingering Concerns

Six years have passed since the U.S. government publicly acknowledged the U.S. VEP and three years since the passage of statutory reporting requirements, both important steps toward transparency. There are, however, lingering concerns as to the appropriate use of vulnerabilities and the adequacy of Congress's recent efforts to put in place reporting and notice requirements specific to the U.S. VEP. The critiques are wide-ranging and reflect technical, ethical, policy and legal dimensions.[121] This section focuses on the critiques that impact accountability and transparency. These include arguments that the U.S. VEP: (1) lacks key players and perspectives in its decision-making process; (2) excludes wide swath of vulnerabilities from any review under the U.S. VEP's "exceptions" and "exclusions" provisions, including vulnerabilities obtained through NDAs or partner agreements or those used in "sensitive operations"; (3) lacks consistent agency interpretations and processes for defining and identifying vulnerabilities that require submission to the U.S. VEP; (4) is inconsistent with industry disclosure standards and expectations; and (5) lacks an enforcement or accountability mechanism to assess whether the process is being followed and to impose consequences for non-compliance. While cataloging these lingering gaps, this section also will delve into the broader challenges that limit the vitality of external oversight efforts when the topic is governmental use of vulnerabilities and cyber capabilities more broadly.[122]

---

[119] Intelligence Authorization Act for Fiscal Year 2018, S. 1761, 115th Cong. § 607 (2017); Intelligence Authorization Act for Fiscal Year 2018, H.R. 3180, 115th Cong. § 107 (2017). The provision was eliminated from the version of the bill eventually enacted as part of the NDAA for FY2020.

[120] *See infra* Section III.B (explaining why the IC IG is well-suited to the vulnerability oversight task).

[121] *See generally supra* note 22 and sources cited therein.

[122] Similar concerns echo in the context of technology-enabled tools and capabilities, which push the bounds of the idea of civilian control and congressional oversight. *See, e.g.*, Ashley Deeks,

1. Inadequate Players and Perspectives

One of the most common critiques of the U.S. VEP is that it lacks key players and perspectives in its decision-making process. As a result, the process gives inadequate consideration to non-governmental interests, most notably the commercial interests of industry, the privacy interests of consumers, and the security interests of other nations. This critique is reflected in both the composition of the ERB (the players at the U.S. VEP table) and a calculation of the equities (with the governmental-equities vastly outnumbering the industry- and public-facing equities).

With regard to the players, the U.S. VEP lacks any formal input or participation mechanism that reflects the interests of industry, foreign partners, or the public. Notably absent from the list of ERB permanent members are the Departments of Education, Health and Human Services, and Transportation, all agencies that oversee sectors where the companies are frequent victims of vulnerability-enabled cyber operations.[123] And while the ERB includes the U.S. Department of Commerce, arguably able to represent industry perspectives, and the U.S. Department of State, arguably able to represent the interests of foreign partners and the international community, scholars have flagged these channels as inadequate and ineffective substitutes.[124] A similar problem exists regarding the lack of representation of the interests of the public in a safe, secure, and accessible internet and in consumer privacy. Although the policy's

Secrecy Surrogates, 106 VA. L. REV. 1395, 1413–16 (2020) (explaining why congressional committees are "less than fully effective overseers" of intelligence and defense matters) [hereinafter Deeks, *Secrecy Surrogates*]; Amy B. Zegart, The Domestic Politics of Irrational Intelligence Oversight, 126 POL. SCI. Q. 1, 9-24 (2011) (explaining challenges of congressional oversight in intelligence operations); *see also* Rebecca Crootof & BJ Ard, *Structuring Techlaw,* 34 HARV. J.L. & TECH. 347, 349–50 (2021) (citations omitted) (explaining that "fundamental challenge of techlaw is not how to best regulate novel technologies, but rather how to best address familiar forms of legal uncertainty in new sociolegal contexts," and proposing a framework for doing so).

[123] U.S. VEP, *supra* note 9, Section 4.1 (listing ERB members). Other conceivable channels for these perspectives would be through the VEP's process for temporary ERB participants which permits—but does not require—participation by other government agencies and entities that "demonstrate[e] responsibility for, or identify[] equity in, a vulnerability under deliberation." As noted earlier, it is not clear how such temporary members receive notice that a vulnerability has been submitted to the VEP for consideration if they are not on the ERB's permanent member list, other than by express invitation of the Executive Secretariat.

[124] *See, e.g.,* Sharon Bradford Franklin & Andi Wilson, *Rules of the Road: The Need for Vulnerabilities Equities Legislation*, LAWFARE (Nov. 22, 2017) (noting that participants in ERB process are "heavily slanted toward the intelligence and law enforcement communities"); *see also* SCHWARTZ & KNAKE, *supra* note 22.

purpose includes a commitment to "prioritize the public's interest in cybersecurity,"[125] there is no dedicated representative for the public nor a mechanism to gather the public's perspective.[126]

The lack of formal representation on the review board is exacerbated by the high number of equities favoring national security, intelligence, and law enforcement interests when compared to the single equity listed in the commercial and international categories.[127] As cataloged by other scholars, the equities listed in Annex B are dominated by governmental interests while only a smattering provide for industry-related interests.[128] Microsoft and Mozilla have been vocal in flagging the lack of industry input and the impact that lack of input has on the review process. In response to the WannaCry attack, Microsoft's CEO Brad Smith urged:

> [T]he governments of the world should treat this attack as a wake-up call. They need to take a different approach and adhere in cyberspace to the same rules applied to weapons in the physical world. We need governments to consider the damage to civilians that comes from hoarding these vulnerabilities and the use of these exploits. This is one reason we called in February for a new "Digital Geneva Convention" to govern these issues, including a new requirement for governments to report vulnerabilities to vendors, rather than stockpile, sell, or exploit them.[129]

Of related concern, is the lack of any "citizenry-oriented"[130] considerations or equities in the U.S. VEP, leading digital rights advocates to flag significant privacy and civil liberties concerns.[131] The quantitative disparity in the equities

---

[125] U.S. VEP, *supra* note 9, Section 1.

[126] The lack of permanent member representation in the ERB from the Federal Trade Commission (representing data privacy and data security interests) and the Federal Communications Commissions (representing the interests of the telecommunications industry and consumer security) creates the impression that the public's interest may not be at the forefront of VEP considerations. Polley, *supra* note 22, at 97–98.

[127] U.S. VEP, Annex B.

[128] *See* Polley, *supra* note 22, at 98 (noting "a deficiency in the VEP's consideration of public- or social good-oriented equities").

[129] Smith, *supra* note 2; Dixon, *supra* note 21.

[130] Polley, *supra* note 22, at 98.

[131] For a summary of privacy and civil liberties concerns relating to the U.S. VEP, see the pleadings and other materials related to the FOIA litigation pursued by the Electronic Frontier Foundation (EFF) (EFF v. NSA, Case No.: 14-cv-03010-RS, February 18, 2016, https://www.eff.org/document/vep-foia-effs-xmsj-and-opp) and by the Electronic Privacy Information Center (EPIC) (EPIC v. NSA: NSPD-54 Appeal, https://epic.org/foia/nsa/nspd-54/appeal/.

recognized in Annex B leads to conclusions that the decision-making process is biased toward vulnerability retention and non-disclosure.

This potential for retention bias is further reflected in the agency that provides the administrative home for the U.S. VEP: the National Security Agency serves as the Executive Secretariat for VEP decisions, "acting at all times under the authority, direction, and control of the Secretary of Defense."[132] As noted by Sven Herpig, "institutional setup is one of the toughest challenges in designing" equities processes,[133] which counsels that the selection of the lead agency should be unbiased to the greatest extent possible. While the NSA is well-staffed and resourced to serve as the U.S. VEP's administrative home, its origins in the defense and intelligence domains create distrust within the private sector and perceptions of a bias toward retention.[134] The combination of a defense-oriented administrative home for the U.S. VEP and the lack of industry representation on the ERB has fomented distrust within the private sector, and the decision to retain knowledge of the EternalBlue vulnerability for five years after discovering it and using it for intelligence exploits badly damaged the U.S. government's relationship with private sector entities.[135] Despite the NSA's recent efforts to rebuild that trust, the residue from earlier failures lingers.[136]

---

[132] U.S. VEP, *supra* note 9, Section 4.2.

[133] HERPIG, WEIGHING, *supra* note 22. For the counter-view and support for the idea that the NSA should maintain its role as VEP Executive Secretariat, see Susan Hennessey, *Vulnerabilities Equities Reform That Makes Everyone (And No One) Happy*, LAWFARE (July 8, 2016), https://www.lawfaremedia.org/article/vulnerabilities-equities-reform-makes-everyone-and-no-one-happy ("But for the 'close calls' where the subtle influence of particular roles might actually impact the outcome, the NSA, FBI, and DOD have far more complex equities and a deeper base of expertise.").

[134] *See, e.g.*, SCHWARTZ & KNAKE, *supra* note 22, at 15 ("Even if the NSA can internally find a means to manage this process in an evenhanded manner, there is still an appearance of conflict that raises unnecessary questions about the impartiality of the VEP.").

[135] Newman, *supra* note 1; *see also* Ellen Nakashima & Craig Timberg, *NSA Officials Worried About the Day Its Potent Hacking Tool Would Get Loose. Then it Did*, WASH. POST (May 16, 2017), https://wapo.st/3HS6fRI. The tendency to withhold vulnerabilities did not cease with news of the WannaCry and NotPetya attacks or the publication of the U.S. VEP. Ellen Nakashima & Rachel Lerman, *FBI Held Back Ransomware Decryption Key from Businesses to Run Operation Targeting Hackers*, WASH. POST (Sept. 21, 2021), https://www.washingtonpost.com/national-security/ransomware-fbi-revil-decryption-key/2021/09/21/4a9417d0-f15f-11eb-a452-4da5fe48582d_story.html.

[136] Ellen Nakashima, *The Cybersecurity 202: Here's Why NSA Rushed to Expose a Dangerous Computer Bug,* WASH. POST (Feb. 6, 2020), https://wapo.st/49racbW; Sean Lyngaas, *NSA Says it Found New Critical Vulnerabilities in Microsoft Exchange Server*, CYBERSCOOP (Apr. 13, 2012), https://bit.ly/42ydaZW. Even when the government would like to share cyber information, a number of challenges relating to classified information and the protection of sources and

2. Cavernous Exceptions and Exclusions

The U.S. VEP also is criticized for excluding a wide swath of vulnerabilities from any review under its exceptions and exclusions provisions.[137] As described more fully above, these include vulnerabilities that are purchased[138] by the government —rather than developed or discovered by it—, vulnerabilities that are subject to partner agreements with exclusivity clauses or non-disclosure agreements[139] —which also affects purchased vulnerabilities—, and vulnerabilities that are involved in "sensitive"[140] military or intelligence operations. The perception is that a wide swath of vulnerabilities are not submitted for consideration under the process, thus evading the oversight and accountability checks the process was intended to provide. The breadth of the exceptions and exclusions means, in practice, that a number of vulnerabilities never reach the balancing of equities stage.

Perhaps the most notorious example of the U.S. VEP's purchasing loophole comes from the fight between Apple and the FBI over unlocking the phone of the San Bernardino shooter. Shortly before a court hearing, the U.S. government revealed that a third party had assisted the FBI in unlocking the phone. It was later revealed that the U.S. government paid close to $1.3 million for the vulnerability that would unlock the phone.[141] Possibly even more concerning was when the government explained that because the vulnerability

---

methods, inhibits the ability to quickly disseminate the information to partners in the private sector. *See* Knake, *Sharing*, *supra* note 38.

[137] U.S. VEP, *supra* note 9, Section 5.4 & Annex C.

[138] Rhys Dipshan, *The Federal Policy Loophole Supporting the Hacking-for-Hire Market*, SLATE (June 20, 2018), https://bit.ly/3SS5eQ3; Thompson, *supra* note 22. For a summary of the purchasing loophole, see Greenberg, *supra* note 58.

[139] U.S. VEP, *supra* note 9, at Section 5.4; *see also* Healey, *Zero-Day Vulnerabilities*, *supra* note 21, at 10 (suggesting there may be a loophole when the U.S. uses vulnerabilities provided by allies or other foreign partners).

[140] U.S. VEP, *supra* note 9, at Section 5.4. The term "sensitive operations" is not defined in the VEP. Presumably, however, these operations include joint operations with allies or other partners. "[I]f these partners have a vulnerability that they are actively exploiting (or planning to exploit), it is possible that the US Government may need to abide by any disclosure or retention restrictions put in place by these counterparts—even if it goes against an ERB adjudication decision." Polley, *supra* note 22, at 24. Others have pointed out the ability to avoid the ERB review process by labeling any law enforcement or intel operation as "sensitive." Crocker, *supra* note 60 ("And exempting vulnerabilities involved in 'sensitive operations' seems like an exceptionally wide loophole, since essentially all offensive uses of vulnerabilities are sensitive.").

[141] Eric Lichtblau & Katie Benner, *F.B.I. Director Suggests Bill for iPhone Hacking Topped $1.3 Million*, N.Y. TIMES (Apr. 21, 2016), https://www.nytimes.com/2016/04/22/us/politics/fbi-director-suggests-bill-for-iphone-hacking-was-1-3-million.html?smid=url-share.

was purchased, and not discovered by the government, it was not submitted to the U.S. VEP's equities balancing process.[142] The second data point comes from the classified budget information leaked as part of the Snowden documents: according to the leaked documents, the NSA's budget for 2013 included $25.1 million for "additional covert purchases of software vulnerabilities."[143]

There is a related secondary effect resulting from the U.S. VEP's purchasing loophole. It has been blamed for creating an international vulnerabilities market, with a group of particularly ominous players engaged in a subsidiary market for zero-day vulnerabilities.[144] The development and perpetuation of such markets by governmental demand for vulnerabilities and

---

[142] Eric Tucker, *FBI Says It Won't Disclose How It Accessed Locked iPhone*, AP NEWS (Apr. 27, 2016), https://apnews.com/united-states-government-3ed26fcb4eb0453ea8de7f0cbbebf2bc; *see also* Healey, *Zero-Day Vulnerabilities, supra* note 21, at 13 (describing how the FBI's purchase of a vulnerability-based tool to unlock an iPhone 5C was excluded from the VEP).

[143] Brian Fung, *The NSA Hacks Other Countries by Buying Millions of Dollars' Worth of Computer Vulnerabilities*, WASH. POST (Aug. 31, 2013). More recent data is unavailable because such budgets tend to be classified. For an estimate of how many vulnerabilities could be purchased for that amount and the implications for the number of vulnerabilities retained, *see* Healey, *Zero-Day Vulnerabilities, supra* note 21, at 11. Based on those calculations and assuming the FBI and CIA also purchase vulnerabilities, the annual budget allocation may be closer to $75 million. *Id.* More recent vulnerability pricing information can be found in a 2024 report by Google. GOOGLE TAG, BUYING SPYING, *supra* note 7, at 24–25 (providing pricing models for commercial spyware packages from key vendors).

[144] Dipshan, *supra* note 138; *see also* PERLROTH, *supra* note 2, at xiv, 39–40 (describing U.S. government's unintended role, through its development and use of cyber capabilities, in creating a market for vulnerabilities). Perlroth describes the vulnerability market's origins, its pricing structure, its codes of professional conduct and deal-making norms, its sellers, its buyers, and the cybersecurity firms and researchers that attempt to study it. She explains how the price of a vulnerability went from $400 in the early days of the market to $4,000 only three years later to around $50,000 five years on. Indeed, the owner of a player in the marker, iDefense told the author that "the first thousand bugs iDefense paid $200,000 for in the first eighteen months of the program would have cost $10 million today [2020]." *Id.* at 40. For more detailed accounts of the USG's purchasing efforts, particularly the NSA's purchasing of zero day vulnerabilities, see SHANE HARRIS, @WAR: THE RISE OF THE MILITARY-INTERNET COMPLEX 102, 119 (2015); Kim Zetter, *Hacking Team Leak Shows How Secretive Zero-Day Exploit Sales Work*, WIRED (July 24, 2015), https://bit.ly/3UFOAoh; LILIAN ABLON, MARTIN C. LIBICKI & ANDREA GOLAY, MARKETS FOR CYBERCRIME TOOLS AND STOLEN DATA: HACKERS' BAZAAR (2014); *see also* Sven Herpig & Alexandra Paulus, *The Pall Mall Process on Cyber Intrusion Capabilities*, LAWFARE (Mar. 19, 2024), https://www.lawfaremedia.org/article/the-pall-mall-process-on-cyber-intrusion-capabilities#:~:text=The%20process%20brought%20together%20states,commercial%20cyber%20intrusion%20capability%20ecosystem (describing "the leading role that governments play in fueling this currently out-of-control ecosystem" for commercial spyware and cyber-intrusion capabilities more broadly). "As long as there is demand for surveillance capabilities, there will be incentives for CSVs to continue developing and selling tools, perpetrating an industry that harms high risk users and society at large." GOOGLE TAG, BUYING SPYING, *supra* note 7, at 40.

the willingness of governments to pay steep prices for zero days undercuts efforts to strengthen international norms of responsible behavior in cyberspace. A February 2024 report issued by Google's Threat Analysis Group stated that commercial spyware vendors—the entities from which governments purchase vulnerabilities—"are behind half of known zero-day exploits targeting Google products as well as Android ecosystem devices."[145] In sum, "[i]f there is going to be mischief in the VEP process, it will be in the overuse of these exceptions to divert hacking tools away from the VEP review" and to place the government's use of vulnerabilities and other cyber-intrusion capabilities outside the reach of the relevant oversight authorities.[146]

3. Inconsistent Agency Interpretations and Submission Criteria

A third concern is that the U.S. VEP lacks consistent agency interpretations and processes for defining and identifying vulnerabilities that require submission to the U.S. VEP. The unclassified charter does not define or provide examples of what types of governmental interests may present "demonstrable, overriding interest," which contributes to further confusion. Thus, agencies may be making inconsistent decisions as to which vulnerabilities are excepted or excluded from the process. For example, how precisely are the categories of "partner agreements" and "sensitive operations" outlined in classified Annex C? Is there variation in practice between the CIA, FBI, and NSA in how they define "sensitive operations"? While the U.S. VEP explains that lists of excepted vulnerabilities will be provided in ERB meetings, questions remain about each member's process or criteria for concluding that a vulnerability should be excepted.

The statutory reporting requirements attempted to get at this concern by requiring the DNI to submit a report on the process used to make VEP determinations at the entity level, and to provide updates when there are changes in the process. The publication of this information, however, is lacking despite the requirement for an unclassified form of the report.[147] Pairing the lack of consistent agency criteria for when a vulnerability meets the threshold submission requirements with the exclusions and exceptions noted above leads to further doubts as to the viability of the U.S. VEP as an effective balancing

---

145 GOOGLE TAG, BUYING SPYING, *supra* note 7, at 2.
146 Richardson, *supra* note 22.
147 50 U.S.C. § 3316a(b)(3). *See infra* Section III.5 (describing lack of public reports).

framework. These oversight concerns also lead to questions on the size of the U.S. government's vulnerability stockpile.[148]

4. Conflicting Industry Disclosure and Information Sharing Expectations

The fallout from a slew of high-profile cyber incidents in the last few years, including SolarWinds, Microsoft Exchange, Colonial Pipeline, and Kaseya VSA provided compelling reminders that government and private sector networks are intimately connected and inter-dependent, and that the need for timely and accurate information sharing about vulnerabilities is critical.[149] The much-heralded 2020 Cyberspace Solarium Commission Report highlighted the need to "operationalize cybersecurity collaboration with the private sector," urging the U.S. government and industry to develop "a new social contract of shared responsibility to secure the nation in cyberspace."[150] At the core of this new

---

[148] This question has been around since the beginning, *see* Healey, *Zero-Day Vulnerabilities, supra* note 21, at 10. Accounts vary and the government's stated percentages are contested. *See, e.g.,* JAIKARAN, *supra* note 29, at 3 ("The National Security Agency Director testified that the government discloses around 93% of identified vulnerabilities to the affected technology company through the VEP.")

[149] For example, the U.S. government's cyber threat detection systems failed to detect, identify, or halt the SolarWinds compromise. Rather, a private company, FireEye, alerted the U.S. government to the breach. *Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims with SUNBURST Backdoor*, FIREEYE (Dec. 13, 2020), https://perma.cc/X87G-F9WN; Sean Lyngaas, *FireEye Says Hackers Stole its Red-Team Tools, Suggests State-Sponsored Group is to Blame*, CYBERSCOOP (Dec. 8, 2020), https://cyberscoop.com/fireeye-says-hackers-stole-its-red-team-tools-suggests-state-sponsored-group-is-to-blame/. Of further note in the lack of information sharing and distrust space, at least one private company identified the breach several months before FireEye but decided not to share that cyber threat intelligence with other companies or the federal government. *See* Robert Knake, *Most Tools Failed to Detect the SolarWinds Malware. Those That Did Failed Too*, COUNCIL ON FOREIGN RELS. (Jan. 28, 2021), https://perma.cc/A9N2-Y9EC ("While the failure of the cybersecurity industry to detect the campaign after years of relentlessly hyping their capabilities against these actors is troubling, what is even more concerning is that at least one vendor is claiming that they detected and stopped the campaign. In a blog post, Palo Alto Networks, in a bit of a humble brag, noted that they had detected the activity on their own network, thwarted the attack, distributed signatures to protect their customers, but had not realized that it would turn out to be a big deal.") (linking to Nikesh Arora, *Palo Alto Networks Rapid Response: Navigating the SolarStorm Attack*, PALO ALTO NETWORKS (Dec. 17, 2020), https://www.paloaltonetworks.com/blog/2020/12/solarwinds-statement-solarstorm/.

[150] U.S. CYBERSPACE SOLARIUM COMMISSION FINAL REPORT 96 (2020) [hereinafter CSC FINAL REPORT 2020]. Echoes of this earlier call for a new social contract can be found in the 2023 NAT'L CYBERSECURITY STRATEGY, *supra* note 88, and a 2024 Foreign Affairs article co-authored by the inaugural National Cyber Director, Chris Inglis & Harry Krejsa, *The Cyber Social Contract: How to Rebuild Trust in a Digital World*, FOREIGN AFFS. (Feb. 21, 2022), https://www.foreignaffairs.com /articles/united-states/2022-02-21/cyber-social-contract.

social contract will be the need to share information about cyber threats and vulnerabilities.[151]

Despite this recognition of a shared and connected public-private cyber fate, there is a long simmering frustration among industry players when they hear calls to share and collaborate. That frustration is the result of a perceived, and arguably actual, discrepancy between the standard the U.S. government applies to itself for sharing vulnerability information—"retain or disclose"—and the expectations the U.S. government places on industry to share such information—"always disclose." This dual standard is reflected in the different categories of vulnerability disclosure policies described above.[152] The inconsistent expectations and presumptions may account for the "collective groan from those in the industry" that meets calls for public-private partnerships and shared responsibility for cybersecurity.[153] Complaints abound from the private sector regarding how and the extent to which information flows between government agencies and industry. Rather, it seems to be a one-way conduit; industry shares information with government and the government says thank you, but does not reciprocate. At the base of this critique is distrust over sharing cyber threat and vulnerability information. Whether warranted or not, the U.S. government has a reputation for failing to share or disclose the cyber-intrusion related information it possesses, thus contributing to the view that the U.S. government is stockpiling vulnerabilities.[154]

5. Ineffective Enforcement Mechanisms and Accountability Checks

A final and persistent critique is that the U.S. VEP lacks an enforcement mechanism or public accountability check. There is no mechanism to ensure

---

[151] Despite the general feelings of frustration and distrust when it comes to vulnerability disclosure, there are a number of government-sharing efforts that seek to contribute to the security of the larger cyber ecosystem and that have been well-received by industry. These include CISA's Cybersecurity Alerts & Advisories website (CISA: CYBERSECURITY ALERTS & ADVISORIES, https://www.cisa.gov/news-events/cybersecurity-advisories (last visited Apr. 13, 2024)), and CISA's maintenance of the Known Exploited Vulnerabilities Catalog (CISA: KNOWN EXPLOITED VULNERABILITIES CATALOG, https://www.cisa.gov/known-exploited-vulnerabilities-catalog (last visited Apr. 13, 2024)).

[152] *See supra* Section I (grouping vulnerability disclosure policies based on the status of the discovering entity).

[153] RICHARD CLARKE & ROBERT KNAKE, THE FIFTH DOMAIN: DEFENDING OUR COUNTRY, OUR COMPANIES, AND OURSELVES IN THE AGE OF CYBER THREATS 89 (2019); *see also* Kristen Eichensehr, *Public-Private Cybersecurity*, 95 TEX. L. REV. 467, 484 (2017) (considering incentive mismatch, with private companies favoring disclosure to allow for patching and the government wanting to keep the vulnerability secret).

[154] Healey, *Zero-Day Vulnerabilities*, *supra* note 21, at 14.

the equity-balancing decision-making process is being followed and there is no enforcement lever for imposing consequences for non-compliance. These concerns about the U.S. VEP reflect the broader constitutional unease that characterizes the government's use of vulnerability-enabled intrusion tools. The need for secrecy and speed required to carry out effective vulnerability-enabled operations hinder the usual democratic checks.[155] Despite the recent addition of statutory reporting requirements relating to the U.S. VEP,[156] the unease hangs about given their limited and feeble scope. The requirements apply to only some of the entities that participate in the U.S. VEP.[157] The reporting goes only to the intelligence committees.[158] Moreover, the requirements lack the detail and granularity that would provide the level of information necessary to effectively engage the vulnerability oversight task.[159]

The feebleness of the reporting requirements is exacerbated by the disjointed and fractured legislative committee structure for oversight of the U.S. government's cyber-related activities.[160] There are no committees focused

---

[155] Goldsmith & Waxman, *supra* note 20, at 18 (describing how light footprint warfare, including through the use of cyber-intrusion tools, may be a "bug for U.S. democracy, since the stealthy features mean that public debate and political checks—which reduce error as well as excess, and promote legitimacy—function ineffectively"); *see also supra* note 20 and sources cited therein.

[156] *See supra* Section II.B (describing statutory reporting requirements set forth in 50 U.S.C. § 3316a)

[157] 50 U.S.C. § 3316a(b)(1)(A) (limiting process and criteria reporting requirements to each "element of the intelligence community").

[158] 50 U.S.C. § 3316a(b) & (c) (limiting reporting to intelligence committees).

[159] 50 U.S.C. § 3316a(c)(1) (limiting the data requested in the annual reports to "(A) the number of vulnerabilities submitted for review under the Vulnerabilities Equities Process; (B) the number of vulnerabilities described in subparagraph (A) disclosed to each vendor responsible for correcting the vulnerability, or to the public, pursuant to the Vulnerabilities Equities Process; and (C) the aggregate number, by category, of the vulnerabilities excluded from review under the Vulnerabilities Equities Process, as described in paragraph 5.4 of the Vulnerabilities Equities Policy and Process document."). The unclassified appendix to the report describes slightly different categories: "(A) the aggregate number of vulnerabilities disclosed to vendors or the public pursuant to the Vulnerabilities Equities Process; and (B) the aggregate number of vulnerabilities disclosed to vendors or the public pursuant to the Vulnerabilities Equities Process known to have been patched." 50 U.S.C. § 3316a(c)(2). Scholars have noted the importance of more precise information about how the process works. *See, e.g.*, HERPIG, WEIGHING, *supra* note 22, at 27–28 (listing specific questions that should be included in legislative reporting efforts); Thompson, *supra* note 22 ("It is critical that the reporting process clarify the number of vulnerabilities out there, because size matters. Dozens? Hundreds? Thousands? The importance of a transparent process directly correlates with the size of the 'stockpile' because size increases the threat model.")

[160] *See* Carrie Cordero & David Thaw, *The Cyberspace Solarium Commission's Mandate to Fix Congressional Oversight*, LAWFARE (Mar. 18, 2020), https://bit.ly/3HUJrRy; Carrie Cordero & David Thaw, *Rebooting Congressional Cybersecurity Oversight*, CTR. FOR A NEW AM. SEC. (Jan. 30,

solely or entirely on cyber matters. Rather, oversight of cyber-related responsibilities and capabilities is divided among many committees and sub-committees. As each committee views the cyber issue only through the narrow lens before it, Congress, as an oversight body, fails to grasp the larger cyber framework and lacks an appreciation for how the defensive and offensive pieces fit together. The structural concern is intensified by a general lack of technological savvy or basic cyber literacy, within the committees charged with oversight.[161] Research into the skill sets and expertise of the relevant committee staff demonstrates "a serious dearth of technical expertise among the staffers."[162] Ashley Deeks provides the challenge in stark terms: "It is far from clear that members or staffers have the technological sophistication necessary to provide deep oversight over programs involving complicated electronic surveillance, cyber, or artificial intelligence technologies."[163]

2020), https://bit.ly/498IYHr ("[T]he lack of a coordinating function among these committees limits Congress's ability to obtain a comprehensive picture of the cybersecurity problem."); CSC FINAL REPORT 2020, *supra* note 150, at 35 (disjointed nature of current committee structure "prevents Congress from effectively providing strategic oversight of the executive branch's cybersecurity efforts or exerting its traditional oversight authority for executive action and policy in cyberspace").

[161] *See, e.g.*, Zach Graves & Daniel Schuman, *The Decline of Congressional Expertise Explained in Ten Charts*, TECHDIRT (Oct. 18, 2018), https://bit.ly/42Bs7KH ("When Mark Zuckerberg was called to testify earlier this year, the world was shocked by Congress's evident lack of basic technological literacy."); Emily Stewart, *Lawmakers Seem Confused about What Facebook Does—and How to Fix it*, VOX (Apr. 10, 2018), https://bit.ly/3uvgcSk ("Many of the lawmakers' questions suggested they're still trying to understand the basics of how the [Facebook] platform works."); Cristiano Lima-Strong, *Silicon Valley's Top Scholars Being Ignored in AI Debate*, WASH. POST (Feb. 8, 2024), https://www.washingtonpost.com/politics/2024/02/08/silicon-valleys-khanna-top-scholars-being-ignored-ai-debate/ (describing remarks from Representative Ro Khanna that academics who have spent their lives studying AI are "getting short shrift" and that "academic expertise was being ignored in Washington" as Congress considered AI-related legislation).

[162] Jenna McLaughlin, *Congress May Lack Technical Expertise to Properly Investigate Russian Hacking*, THE INTERCEPT (Feb. 28, 2017), https://bit.ly/3wfqvdO (concluding that committee staff tend to be "lawyers, policy wonks, and budget experts" not experts in "coding, information security, and attribution").

[163] Deeks, *Secrecy Surrogates*, *supra* note 122, at 1415. There are, however, some congressional officeholders who prove the exception to rule, including Senator Angus King, Representative Mike Gallagher, former Representative Jim Langevin and former Senator Ben Sasse (all members of the Cyberspace Solarium Commission). As of March 2024, only Senator King plans to seek reelection. ANGUS FOR MAINE, https://angusformaine.com/ (last visited Apr. 13, 2024) (2024 senate campaign website); Ally Mutnick & Stephanie Murray, *Langevin Won't Seek Reelection, Opening Rhode Island Seat*, POLITICO (Jan. 18, 2022), https://www.politico.com/news/2022/01/18/langevin-reelection-rhode-island-527311; Stephen Neukam, *Sasse Officially Leaves Senate*, THE HILL (Jan. 8, 2023), https://thehill.com/homenews/3804549-sasse-officially-leaves-senate/; Todd Richmond, *Gallagher Announces He Won't Run for US House Seat in 2024*, PBS WISCONSIN (Feb. 11, 2024), https://pbswisconsin.org/news-item/gallagher-announces-he-wont-run-for-us-house-seat-in-2024/.

Finally, while the statutory mandates for reporting now exist, there remains the challenge of determining whether the required reports are being prepared or submitted. Despite a commitment in the U.S. VEP charter and statutorily imposed requirements to provide annual reports to Congress, the reports appear to be absent. While the classification level of the reports may account for some of the difficulty here, Congress added a requirement in 2022 that an unclassified annex should accompany the annual reports.[164] It seems the unclassified annex has not provided a meaningful level of transparency. To date, the reports do not appear to be publicly available on any government website, and there has been no media reporting on such reports. As such, it remains difficult to assess whether these classified reports are finding their way to the appropriate congressional committee or whether the unclassified annexes are being made available for public review as required.[165]

Despite recent efforts to publish vulnerability equities policies and to establish reporting requirements, the stockpiling concerns linger. We must develop a way to accommodate two trends pulling in separate directions: acknowledging that vulnerabilities are "here to stay"[166] as a legitimate and

---

[164] Consolidated Appropriations Act, 2022, Pub. Law. 117-103, § 307, 136 Stat. 49, 966 (amending 50 U.S.C. 3316a(c) by adding at the end the following: "(4) PUBLICATION. —The Director of National Intelligence shall make available to the public each unclassified appendix submitted with a report under paragraph (1) pursuant to paragraph (2).").

[165] My own efforts to confirm the submission of these reports have come up short. A review of the Annual Statistical Transparency reports from 2000-2023, all of which have been issued since the NDAA for FY 2020 mandated reporting on the U.S. VEP and could have provided a "non-duplication" pathway for reporting, yielded no mention of the VEP. OFF. OF THE DIR. OF NAT'L INTEL., ANN. STAT. TRANSPARENCY REP. REGARDING THE INTEL. CMTY.'S USE OF NAT'L SEC. SURVEILLANCE AUTHORITIES FOR CALENDAR YEAR 2022 (2023); OFF. OF THE DIR. OF NAT'L INTEL., ANN. STAT. TRANSPARENCY REP. REGARDING THE INTEL. CMTY.'S USE OF NAT'L SEC. SURVEILLANCE AUTHORITIES FOR CALENDAR YEAR 2021 (2022); OFF. OF THE DIR. OF NAT'L INTEL., ANN. STAT. TRANSPARENCY REP. REGARDING THE INTEL. CMTY.'S USE OF NAT'L SEC. SURVEILLANCE AUTHORITIES FOR CALENDAR YEAR 2020 (2021). A review of the Annual Threat Assessment reports from 2020 to 2024, which are prepared by the ODNI and other government officials, similarly included no mention of the VEP or vulnerability-related statistics. OFF. OF THE DIR. OF NAT'L INTEL., ANN. THREAT ASSESSMENT OF THE U.S. INTEL. CMTY. FOR CALENDAR YEAR 2023 (2024); OFF. OF THE DIR. OF NAT'L INTEL., ANN. THREAT ASSESSMENT OF THE U.S. INTEL. CMTY. FOR CALENDAR YEAR 2022 (2023); OFF. OF THE DIR. OF NAT'L INTEL., ANN. THREAT ASSESSMENT OF THE U.S. INTEL. CMTY. FOR CALENDAR YEAR 2021 (2022); OFF. OF THE DIR. OF NAT'L INTEL., ANN. THREAT ASSESSMENT OF THE U.S. INTEL. CMTY. FOR CALENDAR YEAR 2020 (2021). There was no mention of the U.S. VEP in the National Defense Authorization Act for Fiscal Year 2024. Pub. L. No. 118-31, 137 Stat. 136 (2023). Efforts by other researchers also have come up short. *See* Polley, *supra* note 22, at 29 ("[U]nable to locate any of the unclassified annual reports that the VEP charter commits to producing, nor was I able to locate any reference to the classified versions that are supposed to be sent to Congress annually."). My efforts will continue and will form the basis for future research on this topic.

[166] Lubin, *supra* note 12, at 36.

valuable tool in the government's national security toolkit while conceding that the traditional oversight mechanisms are not well-suited to the task. A September 2023 Chatham House report aptly captures the dilemma: the "invisibility of cyber activity is all the more reason for robust independent oversight of these activities."[167] Scholars recognizing this mismatch have identified the need for alternative players to take on the oversight task usually assigned to external players, like the Congress, the courts, and the media.[168] This article proposes an addition to the roster of alternative oversight players, one able to address many of the lingering concerns when the subject of the oversight is the government's use of vulnerabilities: the office of the Inspector General for the Intelligence Community.

III. A VIEW FROM WITHIN THE EXECUTIVE BRANCH: VULNERABILITIES AND THE INSPECTOR GENERAL FOR THE INTELLIGENCE COMMUNITY

The preceding section identified persistent loopholes and oversight challenges implicated by the U.S. government's use of vulnerabilities and the U.S. VEP. The common response to address such concerns tends to include calls for increased congressional reporting requirements and codification of the U.S. VEP.[169] This article offers a different approach, one that considers reforms from within the executive branch. While scholars have contributed extensive work to the tasks of cataloging the areas in need of reform relating to the U.S. VEP, less attention has been given to the mechanisms and entities best suited to accomplish these reforms. As noted above, the usual oversight mechanisms are mismatched to the task when the subject is the U.S. government's use of vulnerabilities for law enforcement, intelligence, and national security purposes. As we consider alternative players able to provide oversight and review, the Office of Intelligence Community Inspector General should be our first stop. This section describes the attributes and characteristics that make this entity

---

[167] SKINGSLEY, *supra* note 11, at 29.

[168] *See* Deeks, *Secrecy Surrogates*, *supra* note 122, at 1395–96 (identifying technology companies, local governments, and foreign allies as "secrecy surrogates" with important advantages over traditional oversight mechanisms); Gil, *supra* note 20, at 105 (explaining how "exogenous forces and actors" beyond the usual congressional and judicial mechanisms can serve a checking function); Alan Rozenshtein, *Surveillance Intermediaries*, 70 STAN. L. REV. 99, 122–49 (2018) (describing potential contributions of technology companies, serving as "surveillance intermediaries," to the oversight function).

[169] *See, e.g.*, Thompson, *supra* note 22 (arguing that without codification "the process is on a perpetually unstable footing and subject to change or revision at any time"); Fidler & Herr, *supra* note 107.

uniquely well-suited to provide accountability and transparency for governmental vulnerabilities programs. It begins with a primer on IGs and a summary of the features that IGs in national security and intelligence entities bring to their oversight tasks.[170] It then zeroes in to profile the IC IG's specific attributes and tools. The section concludes by identifying reform priorities and proposing specific contributions the IC IG should make to the vulnerability and VEP oversight tasks in light of these reforms.

A. A Primer on Inspectors General in the U.S. Government

There are currently more than fourteen thousand employees working in seventy-five offices of inspector general in the U.S. government.[171] They are tasked with serving as "the principal watchdogs of the nation's major federal agencies."[172] While the concept of independent auditors within executive branch agencies has existed since the founding of the country, the position was formalized and expanded in the Inspector General Act of 1978 (IGA).[173] The

---

[170] Detailed and comprehensive accounts of the role of inspectors general in national security and intelligence entities within the federal government can be found in CARMEN R. APAZA, INTEGRITY AND ACCOUNTABILITY IN GOVERNMENT: HOMELAND SECURITY AND THE INSPECTOR GENERAL (Tom Payne & Tom Lansford eds., 2011); JACK GOLDSMITH, POWER AND CONSTRAINT: THE ACCOUNTABLE PRESIDENCY AFTER 9/11 (2012); PAUL C. LIGHT, MONITORING GOVERNMENT: INSPECTORS GENERAL AND THE SEARCH FOR ACCOUNTABILITY (1993); Ryan M. Check & Afsheen J. Radsan, *One Lantern in the Darkest Night: The CIA's Inspector General*, 4 J. NAT'L SEC. L. & POL'Y 247 (2010); Gaudion, *Answering, supra* note 94; Margo Schlanger, *Offices of Goodness: Influence Without Authority in Federal Agencies*, 36 CARDOZO L. REV. 53 (2014); Shirin Sinnar, *Protecting Rights from Within? Inspectors General and National Security Oversight*, 65 STAN. L. REV. 1027 (2013).

[171] COUNCIL OF THE INSPECTORS GEN. ON INTEGRITY AND EFFICIENCY, ANN. REP. TO THE PRESIDENT AND CONG. FISCAL YEAR 2021, at 1 (2022).

[172] HENRY A. WAXMAN, IMPROVING GOVERNMENT ACCOUNTABILITY ACT, H.R. REP. NO. 110–354, at 8 (2007) (Conf. Rep.).

[173] Inspector General Act of 1978, Pub. L. No. 95-452, 92 Stat. 1101 (initially codified at 5 U.S.C. app. §§ 1 et seq, amended, and moved to a new chapter in 2022 now codified at 5 U.S.C. § 401 et seq). The IGA created and currently governs the offices of statutory IGs. Although "[f]inding the roots of the IG Act is like making a geological dig, stripping one layer of explanation off another until the underlying stratum is uncovered," LIGHT, *supra* note 170, at 39. The following sources provide able guides to tracing the history of IG-like positions in the federal government since the country's founding through the passage of the 1978 IGA: MICHAEL HENDRICKS & MICHAEL F. MANGANO, INSPECTORS GENERAL: A NEW FORCE IN EVALUATION (1990); CHARLES A. JOHNSON & KATHRYN E. NEWCOMER, U.S. INSPECTORS GENERAL: TRUTH TELLERS IN TURBULENT TIMES (2020); LIGHT, *supra* note 170; MARK H. MOORE & MARGARET JANE GATES, INSPECTORS GENERAL: JUNKYARD DOGS OR MAN'S BEST FRIEND (Esther Scott ed., 1986); BEN WILHELM, CONG. RSCH. SERV., R45450, STATUTORY INSPECTORS GENERAL IN THE FEDERAL GOVERNMENT: A PRIMER (2023); John Adair & Rex Simmons, *From Voucher Auditing*

IGA fit into a group of legislative efforts, which Paul Light called a "busy season in the search for government accountability."[174] These statutes shared common goals: to ensure robust and accountable executive branch decision-making, to increase transparency of executive branch decision-making, and to bolster Congress's access to information in the hands of executive agencies.[175] To accomplish these objectives, Congress made independence the defining feature of the IG position. It provided IGs with a mandate focused on accountability and independence, as reflected in the dual reporting obligation to the agency head and to Congress; the Act's appointment and removal provisions which were recently strengthened in 2022;[176] the organizational structure and reporting lines of the position;[177] the IG's authority to select

to Junkyard Dogs: The Evolution of Federal Inspectors General, 8 PUB. BUDGETING AND FIN. 91 (1988); Margaret J. Gates & Marjorie F. Knowles, *The Inspector General Act in the Federal Government: A New Approach to Accountability*, 36 ALA. L. REV. 473 (1984); Katheryn E. Newcomer, *The Changing Nature of Accountability: The Role of the Inspector General in Federal Agencies*, 58 PUB. ADMIN. REV. 129 (1998).

[174] LIGHT, *supra* 170, at 11. *See* War Powers Resolution, Pub. L. No. 93-148, 87 Stat. 555 (1973) (codified as amended at 50 U.S.C. §§ 1541–50) (establishing consultation and reporting requirements when the president uses military force in certain circumstances); Ethics in Government Act of 1978, Pub. L. No. 95-521, 92 Stat. 1824 (codified in various U.S. Code provisions at 2 U.S.C. §§ 288, 288a to 288m, 5504; 28 U.S.C. §§ 49, 528, 529, 591 to 598, 1365; 5 U.S.C. § 13101 et seq.) (preventing, identifying, and punishing corruption in government); Civil Service Reform Act of 1978, Pub. L. No. 95-454, 92 Stat. 1111 (codified as amended in scattered sections of 5 U.S.C.) (reforming the federal civil service); Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, 92 Stat. 1783 (codified as amended at 50 U.S.C. §§ 1801-13) (establishing procedures and oversight mechanisms for foreign intelligence collection).

[175] While it is difficult to identify the exact mix of motivations that led Congress to enact the IGA, the act was focused on two broad objectives: "[T]o increase the overall scale and effectiveness of audits and investigative activities . . . and to make these activities visible by assuring that the information developed in audits and investigations reaches the highest levels of departments, the Congress, and the American public rather than being stifled at lower levels of the bureaucracy." MOORE & GATES, *supra* note 173, at 13.

[176] Securing Independence of the Inspector General Act of 2022, Pub. L. No. 117-263, § 5201 et seq, 136 Stat. 3222 (Dec. 23, 2022) (revising provisions as to timing and content of notice to Congress when the president removes a statutory inspector general); *see also* Bob Baurer & Jack Goldsmith *Inspector General Reform in the NDAA,* LAWFARE (Dec. 23, 2022), https://www.lawfaremedia.org/article/inspector-general-reform-ndaa.

[177] Independence is also reflected in the day-to-day organizational and operational aspects of the position. First, the IG reports directly to the head of the agency, or the officer next in rank below the head. *See* 5 U.S.C. § 403(a) (formerly 5 U.S.C. app. 3 § 3(a)) (indicating that, in most instances, IGs report directly to the agency head or high-level member of the secretary's executive team). In addition, the IG has the authority to structure the office, selecting heads of the various departments and hiring and firing staff. *See* 5 U.S.C. § 403(d) (formerly 5 U.S.C. app. 3 § 6) (explaining that IGs may, as necessary, appoint Assistant IGs as well as IGs to head other departments).

activities and to act without interference;[178] and the obligation to make reports available to the general public.[179]

The independence described above is strengthened by the IG's statutorily mandated perch within the executive branch entity and accompanying toolkit. One of the chief advantages of IGs is that they are "ideally situated to detect problems that would otherwise go undetected."[180] IGs serve as an information conduit to congressional committees unable to acquire the information through typical channels.

They fulfill the congressional informing task through a variety of mechanisms, including semiannual reports, implementation updates, fast action reports for particularly egregious violations, specific inquiries from Congress to investigate matters and congressional requests for IG testimony. By design, the agency perch allows the IG to surmount the usual separation of powers

---

[178] The IG receives and identifies work assignments from several sources, including statutory mandate, congressional request, agency head request, or at the IG's own initiative. *See* 50 U.S.C. § 3033; 5 U.S.C. § 416); WILHELM, *supra* note 173, at 7 (explaining that an IG conducts reviews in response to statutory mandate, at the request of Congress or other stakeholders (e.g., the President), or upon self-initiation); JOHNSON & NEWCOMER, *supra* note 173, at 96–97, 132–35 (describing congressional requests for IG action and other interactions between congressional entities and IG offices). Relatedly, the statute gives the IG authority to identify and engage in auditing, investigative, and inspection activities without interference from the department head or others. "Neither the head of the establishment nor the officer next in rank below such head shall prevent or prohibit the Inspector General from initiating, carrying out, or completing any audit or investigation, or from issuing any subpoena during the course of any audit or investigation." 5 U.S.C. § 403(a) (formerly 5 U.S.C. app. 3 § 3(a)). Paul Light identifies this "full authority to undertake whatever audits and investigations deemed necessary" as one of the devices that protects the IG from administrative politics, thus strengthening the IG's powers. LIGHT, *supra* note 170, at 23–24. This protection from interference is a hallmark of the position's independence and fosters the officer's ability to serve public law values. A deeper discussion of the public law values embodied by IGs can be found in Deeks, *Secrecy Surrogates*, *supra* note 122, at 1452–54. There are exceptions to this mandate for IGs located in national security and intelligence agencies. The agency heads in these entities may block IG activities if they relate to certain sensitive topics or national security matters. *See, e.g.,* 50 U.S.C. § 3033(c) (IG for Intelligence Community); 5 U.S.C. § 408(b) (IG for the Department of Defense); 5 U.S.C. § 412(a) (IG for Department of Treasury); 5 U.S.C. § 413(a) (IG for Department of Justice); 5 U.S.C. § 417(a) (IG for Department of Homeland Security); 50 U.S.C. § 3517(b)(3) (IG for Central Intelligence Agency). It is noteworthy, however, that the norm of non-interference is so powerful that even the agency heads with a statutorily granted justification for halting or blocking IG work rarely invoke this prohibition. The most striking example of this may be CIA IG John Helgerson's investigation into CIA detention and interrogation activities. GOLDSMITH, *supra* note 170, at 99–108.

[179] 5 U.S.C. § 405(d). *See generally Inspector General Reports*, OVERSIGHT.GOV, https://bit.ly/485ByDq.

[180] GOLDSMITH, *supra* note 170, at 105; MOORE & GATES, *supra* note 173, at 48.

objections proffered to block legislative, judicial, or public inquiries.[181] These objections are eliminated, or minimized, when the information is sought as part of IG activity. In addition to the special perch, Congress provided IGs with an enviable arsenal of information-gathering tools as part of the IG's charge to keep the agency head, and Congress, "fully and currently informed about problems and deficiencies relating to the administration of such programs and operations and the necessity for and progress of corrective action."[182]

The IG deploys these tools in three principal activities: audits, inspections or evaluations, and investigations, which are more explored more fully in the next section in the specific context of vulnerability oversight.[183] Through the use of their perch and tools, IGs are equipped to gather and disseminate important information to those in policy-making positions, including the relevant legislative committees, agency leadership, and foreign partners. The value of what Ashley Deeks calls "surrogates" is that they have access to highly classified and secret information by virtue of their position or status and thus are able to highlight abusive executive branch actions that otherwise would go unchecked.[184] The IG's special perch and accompanying toolkit allow those in the position to effectively disseminate information to those in policy-making positions, while also providing opportunities to "nudge the Executive toward . . . public law values."[185]

A final feature common to all IGs is the statutory requirement to publish

---

[181] GOLDSMITH, *supra* note 170, at 105 (describing common objections based in claims of classified information, executive privilege, and attorney-client privilege, and obstacles presented by the state secrets and political question doctrines). "Congress in effect delegates its initial oversight function to the [IG], who can quickly gather a much more complete understanding of executive branch activity than Congress itself could have." *Id.* at 105.

[182] 5 U.S.C. § 402(b)(3).

[183] *See* APAZA, *supra* note 170, at 12–14 (comparing the three primary mechanisms by which OIGs accomplish their objectives); WILHELM, *supra* note 173, at 7–9 (describing types of IG reviews and comparing differences in terms of quality standards, scope of analysis, and type of analysis); 5 U.S.C. §§ 406(a), 406(c), 406(d), 406(f) (summarizing tools at IG's disposal).

[184] Deeks*, Secrecy Surrogates*, *supra* note 122, at 1403, 1413–14, 1417.

[185] *Id.* at 1453. Accountability is a hallmark of democratic systems of government, and in the national-security setting, the "relevant subset of public law values includes (1) legal compliance; (2) competence and rationality; (3) holding government decision makers accountable for the decisions that they have made, including by demanding justifications for those decisions; and (4) seeking transparency about government decisions where possible." Moreover, IGs and other secrecy surrogates: "can nudge the Executive toward those public law values by testing whether the Executive appears to be acting in a legal way (or at least not acting in a patently illegal way); whether the Executive appears to be making rational, reasoned decisions based on the secret information it possesses; and whether the Executive is being as transparent as possible, recognizing that some information and acts must necessarily remain secret." *Id.* at 1452–53.

their findings and recommendations for public review.[186] While IGs may not publicly disclose information that is prohibited from disclosure due to classification level or other security-based reasons, most IG reports are published both on the agency's website and the consortium's page, oversight.gov,[187] which features an easily searchable database. The public release of IG reports —even if in redacted form— has the added benefit of subsequent media coverage often followed by congressional attention if Congress missed the importance of the matter when initially receiving the reports. The publication of IG work product helps to remedy the accountability and transparency concerns described above, and also positions IGs to influence internal executive branch policy in a way that Congress often cannot.[188]

B. Welcoming the IC IG to the Oversight Table

The IC IG was a bit of a latecomer to the accountability and oversight party. The position was established in the 2010 Intelligence Authorization

---

[186] 5 U.S.C. § 405(d). For a sampling of the various types of reports, see generally *Inspector General Reports*, *supra* note 179.

[187] *See generally Inspector General Reports*, *supra* note 179; *see also* WILHELM, *supra* note 173, at 19 (describing voluntary origins of and current statutory mandate for oversight.gov).

[188] Shirin Sinnar chronicled the impact that publication of IG reports and recommendations has on the executive branch policy. *See* Sinnar, *supra* note 170, at 1032, 1043 ("The reports drew tremendous media attention, including front-page coverage in major national newspapers, and Congress held several hearings questioning Justice Department officials on the detentions, with members of both parties praising the OIG report."). Examples of IGs influencing internal rules and policies include changes made to the FBI's Foreign Intelligence Surveillance Act (FISA) warrant application process after the DOJ IG's report on the Carter Page/Crossfire Hurricane Investigation; changes made to the CIA's rendition and interrogation programs after the CIA IG's report identified abuses in the program's administration, questioned its efficacy, and doubted the legal basis offered for the program; and the establishment of tighter cybersecurity standards for supply chain vendors after a DoD IG report on vulnerabilities. *See, e.g.*, OFF. OF INSPECTOR GEN., U.S. DEP'T OF JUST., REVIEW OF FOUR FISA APPLICATIONS AND OTHER ASPECTS OF THE FBI'S CROSSFIRE HURRICANE INVESTIGATION (2019) (reviewing FISA application process); Elizabeth Goitein, Andrew G. McCabe, Mary B. McCord & Julian Sanchez, *Top Experts Analyze Inspector General Report Finding Problems in FBI Surveillance*, JUST SEC. (Apr. 27, 2020), https://bit.ly/3wdJdCw; David Kris, *Further Thoughts on the Crossfire Hurricane Report,* LAWFARE (Dec. 23, 2019), https://bit.ly/3SBuN6w; Sinnar, *supra* note 170, at 1047–49 ("Despite the renewed legal authority for enhanced interrogations, the CIA claims that it has not waterboarded any detainees since 2003, and some commentators have credited the inspector general investigation for the cessation of the practice."); OFF. OF INSPECTOR GEN., U.S. DEP'T OF DEF., DODIG-2021-034, SUMMARY OF REPORTS ISSUED REGARDING DEPARTMENT OF DEFENSE CYBERSECURITY FROM JULY 1, 2019 THROUGH JUNE 30, 2020 (2020) (reviewing DoD's cybersecurity standards); Dawn E. Stern & Ryan Carpenter, *Into the Unknown: DOD's Long-Awaited Cybersecurity Rule Leaves Critical Questions Unanswered,* LEXOLOGY (Oct. 5, 2020), https://bit.ly/3UzeTwg.

Act within the Office of the Director of National Intelligence, almost 30 years after the IGA was enacted.[189] Its purpose was to "create an objective and effective office, appropriately accountable to Congress, to initiate and conduct independent investigations, inspections, audits, and reviews on programs and activities within the responsibility and authority of the Director of National Intelligence."[190] Like many of the post-9/11 organizational reforms, it was aimed at harmonizing agency turf battles and it was tasked with coordinating existing IG functions in other intelligence community entities, while also encouraging information sharing outside the usual silos. This section will describe the IC IG's attributes that make it particularly well-equipped for the vulnerability oversight task when paired with the general features described above; these include the ability to engage in audits, inspections, and evaluations; the ability to deploy auditors and others with technical chops and familiarity with the cyber domain; and the ability to take advantage of existing collaborative partnerships. Each of these attributes allows the IG to respond to and overcome lingering concerns about the government's use of vulnerabilities and the ineffectiveness of the current U.S. VEP to meet its objective of balancing the equities at stake in retain-disclose decisions.

1. IG Work Product

As part of the charge to the IC IG to keep the agency head and Congress "fully and currently informed about problems and deficiencies relating to the administration of such programs and operations and the necessity for and progress of corrective action," Congress provided the IC IG with an enviable kit of information-gathering tools.[191] The IC IG utilizes these tools to conduct reviews in three principal categories: performance audits,[192] inspections or

---

[189] Pub. L. No. 111–259, title IV, § 405(a)(1), Oct. 7, 2010, 124 Stat. 2709, codified at 50 U.S.C. § 3033. For a summary of subsequent amendments to the Inspector General Act, including most recently The Securing Inspector General Independence Act of 2022 and the Integrity Committee Transparency Act of 2022, see WILHELM, *supra* note 173, at 3.

[190] 50 U.S.C. § 3033(b).

[191] 5 U.S.C. § 402(b)(3); 50 U.S.C. § 3033 et seq.

[192] The IG also is tasked with "financial audits" which require the IG to hire an independent external auditor to conduct audits of an agency's financial statement. WILHELM, *supra* note 173, at 8. While financial audits are often what IGs are known for, giving rise to the impression of IGs as the bean counters of the federal government, they make up only a small portion of the IC IG work product, and are not the focus of this article. For a comparison of recent reports by categories, see OFF. OF THE INSPECTOR GEN., U.S. INTEL. CMTY., SEMIANNUAL REP. TO THE CONG. FOR APRIL 2023 – SEPTEMBER 2023; OFF. OF THE INSPECTOR GEN., U.S. INTEL. CMTY., SEMIANNUAL REP. TO THE CONG. FOR OCTOBER 2022 – MARCH 2023; and other reports available

evaluations, and investigations.[193] While there is overlap in the categories—and IGs may perform reviews beyond these categories— it is helpful to have a sense of the different quality control standards, the types of analysis, and the scope of analysis anticipated by each review category.

Table: Categories of IG Reviews[194]

	Quality Standards	**Types of Analysis**	**Scope of Analysis**	**Example**
Performance Audit	Generally Accepted Government Auditing Standards (the GAGAS or the Yellow Book[195])	Programmatic analysis (compliance, efficiency and effectiveness, internal control, prospective analysis), may include recommendations	(broad review) Entire agency program or operation	Whether the Executive Director is complying with requirement to provide annual VEP reports to appropriate congressional committees and unclassified annex
Inspection or Evaluation	Quality Standards for Inspection and Evaluation (the	Programmatic analysis (compliance, efficiency and effectiveness,	(narrow review) Specific aspect of a program or operation or specific agency	Whether ERB member agencies are adopting consistent definitions of

at OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE, IC IG REPORTS, https://www.dni.gov/index.php/who-we-are/organizations/icig/icig-publications/icig-all-reports (last visited Apr. 13, 2024).

[193] *See* APAZA, *supra* note 170, at 12–14 (comparing the three primary mechanisms by which OIGs accomplish their objectives); WILHELM, *supra* note 173, at 7–9 (describing types of IG reviews and comparing differences in terms of quality standards, scope of analysis, and type of analysis); 5 U.S.C. app. 3 §§ 4(a), 4(d), 5(a), 6(a), 6(e), 7 (summarizing tools at IG's disposal).

[194] The information included in the table is derived from a similar table in WILHELM, *supra* note 173, at 8.

[195] U.S. COMPTROLLER GEN., GOV'T ACCOUNTABILITY OFF., GOVERNMENT AUDITING STANDARDS (2024), https://www.gao.gov/products/gao-24-106786 [hereinafter YELLOW BOOK] (providing a framework for auditors of government entities and entities that receive government awards, and outlining the requirements for audit reports, professional qualifications for auditors, and audit organization quality management). This source is commonly referred to as generally accepted government auditing standards (GAGAS) or the Yellow Book.

	Blue Book[196])	internal control, prospective analysis), may include recommendations	facility	excluded vulnerabilities, or criteria for identifying vulnerabilities for submission
Investigation	Quality Standards for Investigations (the Silver Book[197]) & relevant Attorney General Guidelines[198]	Non-programmatic, focused on allegations of individual misconduct	(individual review) Actions of an individual employee or contractor	Whether the director of NSA TAO violated the U.S. VEP by refusing to submit qualifying vulnerabilities to the ERB for consideration

Both the performance audit and the inspection/evaluation categories involve reviews of policies, operations, regulations, or legislative implications of a given program, and the reviews tend to fall into two groups: those that assess compliance with applicable laws, regulations, and internal policies and those that assess "how entire programs might be amended or redirected."[199] Topics of recent IC IG reports provide a sense of the breadth of the office's work product: Fiscal Year 2022 Evaluation of the Defense Intelligence Agency; Assessment of All-Source Cyber Intelligence Information Related to Foreign Cyber Threats; Joint Evaluation of the Relationship between the National Security Agency and the United States Cyber Command; and Review of the

[196] COUNCIL OF THE INSPECTORS GENERAL ON INTEGRITY AND EFFICIENCY (CIGIE), QUALITY STANDARDS FOR INSPECTION AND EVALUATION (BLUE BOOK) (2020) (providing framework for inspection and evaluation work by Offices of Inspector General).

[197] COUNCIL OF THE INSPECTORS GENERAL ON INTEGRITY AND EFFICIENCY (CIGIE), QUALITY STANDARDS FOR FEDERAL OFFICES OF INSPECTOR GENERAL (SILVER BOOK) (2012) (providing overall quality framework for managing, operating, and conducting the work of Offices of Inspector General).

[198] U.S. DEP'T OF JUSTICE, GUIDELINES FOR OIGS WITH STATUTORY LAW ENFORCEMENT AUTHORITY (Dec. 2003), http://library.rumsfeld.com/doclib/sp/2847/2003-12-08%20from%20John%20Ashcroft%20re%20Guidelines%20for%20Offices%20of%20Inspector%20General%20with%20Attachments.pdf.

[199] APAZA, *supra* note 170, at 13; *see* JOHNSON & NEWCOMER, *supra* note 173, at 100–04 (describing audit requirements).

Intelligence Community's Compliance with Analytic Tradecraft Standards.[200]

The nature of these reviews allows IGs to engage in evaluative work and to offer recommendations. Only a few years after the 1978 passage of the IGA, scholars were commenting on the growth of evaluative work in the IG portfolio. "The IGs are no longer simply observing program operations to detect isolated problems. Instead, they are proposing changes in procedures that will alter the character of the product or service being delivered, and therefore the value of the program."[201] The impact of IG-related work runs the gambit from cost savings to strengthened internal controls to changes in law, policy, and regulations.[202] The evaluative nature of IG work is best reflected in inspections that "examine the extent to which individual federal programs or installations are complying with applicable laws, regulations, and policies, while other inspections determine how entire programs might be amended or redirected."[203]

2. Technical Chops

In addition, the IC IG can bring technical chops to the vulnerability oversight task as well as familiarity with the executive branch's cybersecurity and information security mandates. This allows it to effectively draw a road map for legislative and agency head attention and action, as well as the attention of non-governmental oversight actors. As noted above, one of the oversight challenges facing legislative entities and the public is an inability to grasp the scope and scale of the executive branch's use of vulnerability-enabled operations and cyber operations more generally. These difficulties stem from a number of institutional challenges, including a lack of cyber literacy or comprehensive understanding of the technologies that allow the use of vulnerability-enabled operations and their tendency to avoid neat categorization into the usual buckets of legal and policy distinction: offense v defense, domestic v foreign, government v industry. The IC IG is able to gap fill for Congress through the reviews it conducts and the reports and testimony

---

[200] OFF. OF THE INSPECTOR GEN., U.S. INTEL. CMTY, SEMIANNUAL REP. TO THE CONG. FOR OCTOBER 2022 – MARCH 2023 17–18, 21–22 (2023).

[201] MOORE & GATES, *supra* note 173, at 29.

[202] JOHNSON & NEWCOMER, *supra* note 173, at 164–65 fig. 6-1.

[203] APAZA, *supra* note 170, at 13; *see also* LIGHT, *supra* note 170, at 19 (noting that ability of IGs to issue not only findings, but recommendations for resolution and improvement based on those findings leads to "broad proposals for change that emerge from audits, investigations, and evaluations.").

it provides. These include annual oversight plans,[204] semiannual reports,[205] implementation updates,[206] fast action reports for particularly egregious violations,[207] joint biennial reports relating to the Cybersecurity Information Sharing Act,[208] annual reports mandated by Federal Information Security Management Act (FISMA),[209] requests for inspector general testimony, and by responding to specific inquiries from Congress.[210] In conducting these reviews and preparing these reports, the IG is able to recruit inspectors and evaluations from other entities with the technical prowess and familiarity to provide technologically accurate and engaged analysis.[211] These reports provide a roadmap rich with guidance on the problem spots and areas in need of urgent attention. Far from a mere compliance exercise, these reports provide a helpful prioritization tool for reviewing the government's use of its vulnerability-enabled operations at a depth and scale unattainable by the usual oversight players.

---

[204] OFF. OF THE INSPECTOR GEN., U.S. INTEL. CMTY., FISCAL YEAR 2024 ANN. WORK PLAN (Sept. 2023), https://www.dni.gov/index.php/who-we-are/organizations/icig/icig-publications/icig-all-reports. The annual plan describes the specific oversight projects the IC IG intends to conduct during the upcoming fiscal year and explains how those activities relate to the top management challenges facing the Intelligence Community. *Id.*

[205] 50 U.S.C. § 3033(k). The IC IG is tasked with preparing semiannual reports summarizing the activities of the Intelligence Community during the immediately preceding six-month period. The reports are to be submitted by the agency head to the relevant congressional committees.

[206] 5 U.S.C. § 3033(e)(2).

[207] 5 U.S.C. § 3033(k)(2).

[208] 6 U.S.C. §§ 1501, 1506(b).

[209] 44 U.S.C. § 3555(b)(1) ("[F]or each agency with an Inspector General appointed under the Inspector General Act of 1978, the annual evaluation required by this section shall be performed by the Inspector General or by an independent external auditor, as determined by the Inspector General of the agency.").

[210] Anticipating the need for congressional support, many offices of inspector general have a division or position dedicated to legislative affairs and tasked with preparing the semi-annual reports and otherwise serving as liaisons between the office and the relevant congressional committees. This role is filled by the Counsel to the IC IG who manages legislative reviews and congressional engagement. OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE, IC IG DIVISIONS AND OFFICES, https://www.dni.gov/index.php/who-we-are/organizations/icig/icig-about-us/icig-divisions (last visited Apr. 13, 2024).

[211] *See* YELLOW BOOK, *supra* note 195, at 100 (explaining resources available to audit the organization including "[h]uman, technological, or intellectual resources from service providers"). The guidance on resources further provides that "[a]ppropriate technological and intellectual resources are obtained or developed, implemented, maintained, and used to enable the operation of the audit organization's system of quality management and the performance of engagements." *Id.* It explains that a "service provider is an individual or organization external to the audit organization that provides a human, technological, or intellectual resource that the audit organization uses in its system of quality management or in performing its engagements."

3. Collaborative Partners

The final attribute that positions the IC IG to provide effective oversight is its participation in—and in some instances, leadership of—existing interagency and intergovernmental models that anticipate the need for cross-agency coordination and foreign partner collaboration. The first example of this attribute is statutorily mandated and tasks the IC IG with coordination among inspectors general of other elements in the intelligence community.[212] The coordination finds a home in the Intelligence Community Inspectors General Forum.[213] The Forum's "mission is to promote and further collaboration, cooperation and coordination among the Inspectors General of the Intelligence Community of the United States."[214] The Forum is chaired by the IC IG, and includes representatives from inspector general offices in the Central Intelligence Agency, Department of Homeland Security, Defense Intelligence Agency, Department of Defense, Department of Energy, Department of State, Department of the Treasury, National Geospatial Agency, National Reconnaissance Agency, National Security Agency, and Federal Bureau of Investigation.[215] Forum members meet quarterly, and activities focus on:

- Supporting the IC IGs in the performance of audits, inspections, evaluations, and investigations within their respective departments and agencies;
- Strengthening the collective role and effectiveness of IGs throughout the Intelligence Community and enhancing the value of IG activities in support of the National Intelligence Strategy; and
- Achieving optimal utilization of resources, to increase efficiency and to avoid duplication of effort among the Inspectors General of the Intelligence Community.[216]

In practice, this mandate provides the IC IG with several tools of potential use in the vulnerability oversight task, particularly in combatting the lingering concern about inconsistent interpretations across agencies and the need for

---

[212] 50 U.S.C. § 3033(h).
[213] 50 U.S.C. § 3033(h)(1)(B).
[214] *IC Inspectors General Forum*, OFF. OF THE DIR. OF NAT'L INTEL., https://www.dni.gov/index.php/who-we-are/organizations/ic-cio/ic-technical-specifications/us-government-agency?id=367 (last visited Apr. 13, 2024).
[215] *Id.*; *see also* 50 U.S.C. § 3033(h)(2)(A).
[216] *Id.*

coordination and deconfliction with coordinated vulnerability disclosure policies. First, the Forum provides a venue for resolving disputes among IG offices as to who should conduct a review. Second, the Forum creates information-sharing channels for reviews of practices that may be of "common interest"[217] to multiple agencies, providing a helpful way to flag issues that are percolating up from the agency level but which may have significant whole of government consequences once the connection is realized. Third, and most relevant for our purposes, through the Forum, the IC IG is able to craft a review that cuts across agencies to provide comparative analysis on topics of common concern. An example would be a review that compares the processes and criteria at various agencies by which vulnerabilities are identified and submitted to the ERB for review. A second example could be a review that examines how the U.S. VEP is impacted by other executive branch mandates, for example, the 2023 executive order on commercial spyware and directives on vulnerability management and disclosures policies.[218]

A second collaborative partner is reflected in the IC IG's role in the Five Eyes Intelligence Oversight and Review Council (FIORC).[219] The FIORC is a partnership that builds on the existing Five Eyes relationship, and includes the following oversight entities: Australia's Office of the Inspector-General of Intelligence and Security;[220] Canada's National Security and Intelligence Review

---

217 50 U.S.C. § 3033(h)(2)(B).

218 *See, e.g.*, Exec. Order No. 14093, Prohibition on the Use by the United States Government of Commercial Spyware That Poses Risks to National Security, 88 Fed. Reg. 18957 (Mar. 27, 2023); OMB MEMO. NO. M-20-32, *supra* note 29; *BOD 20-01*, *supra* note 29; DOD INSTRUCTION 8531.01: DOD VULNERABILITY MANAGEMENT (Sept. 15, 2020). Other areas in need of VEP overlap and deconfliction review include the activities of the Data Privacy Review Court or the Cyber Safety Review Board. *See The Cyberlaw Podcast: Going Deep on Deep Fakes—Plus a Bonus Interview with Rob Silvers on the Cyber Safety Review Board* (Jan. 30, 2024), https://www.lawfaremedia.org/article/the-cyberlaw-podcast-going-deep-on-deep-fakes-plus-a-bonus-interview-with-rob-silvers-on-the-cyber-safety-review-board (featuring an interview with current head of Cyber Security Review Board).

219 CHARTER OF THE FIVE EYES INTELLIGENCE OVERSIGHT AND REVIEW COUNCIL (FIORC) (Oct. 2, 2017), https://www.dni.gov/files/ICIG/Documents/Partnerships/FIORC/Signed%20FIORC%20Charter%20with%20Line.pdf [hereinafter FIORC CHARTER].

220 Australia's Office of the Inspector-General of Intelligence and Security (IGIS) was established in 1986 as an independent statutory office holder charged with reviewing the activities of Australia's six intelligence agencies. Its primary role is to oversee and review the activities of intelligence agencies for legality and propriety and for consistency with human rights. The office's mission is: (i) to be independent and impartial in conducting unbiased assessments; (ii) to be astute and informed of agency activities; (iii) to focus on systemic issues; (iv) to be open in making information public as much as possible through an annual report; and (v) to be influential in helping agencies improve their compliance. Notably, IGIS conducts inspections and reviews of the activities of the Australian Signals Directorate (ASD), the intelligence agency responsible for

Agency[221] and Office of the Intelligence Commissioner;[222] New Zealand's Commissioner of Intelligence Warrants[223] and Office of the Inspector-General of Intelligence and Security;[224] the United Kingdom's Investigatory Powers

collection, analysis, and distribution of foreign signals intelligence. ASD also serves as the national authority on communications and computer security. INSPECTOR-GENERAL OF INTELLIGENCE AND SECURITY, https://www.igis.gov.au/ (last visited Apr. 13, 2024).

[221] Canada's *National Security and Intelligence Review Agency (NSIRA)*, established in 2019, addressed longstanding gaps in Canada's framework for national security accountability and significantly strengthened independent scrutiny of national security and intelligence activities in Canada. The act creating the NSIRA granted statutory powers to access relevant information during its investigations and to conduct independent reviews of government activity. The NSIRA replaced two precursor entities with significantly limited powers of review: the Security Intelligence Review Committee (SIRC) and the Office of the CSE Commissioner (OCSEC). In contrast, the NSIRA is an independent and external review body that reports to Canada's legislative body (Parliament) and has the purview to review all Canadian government national security and intelligence activities to ensure they are "lawful, reasonable, and necessary." The NSIRA also has authority to investigate public complaints about key national security agencies and activities. Relevant to the purposes of this article, NSIRA has a statutory mandate to review the activities of the Communications Security Establishment (CSE), which is responsible for Canada's Equities Management Framework. NATIONAL SECURITY AND INTELLIGENCE REVIEW AGENCY, https://nsira-ossnr.gc.ca/en/home/ (last visited Apr. 13, 2024).

[222] Canada's Office of the Intelligence Commissioner (ICO) was established as part of the reshaping of Canada's national security and intelligence accountability framework. ICO is a separate agency of the Federal Public Administration which operates "at arm's length" from the government as an independent oversight body tasked with supporting the Intelligence Commissioner. The Intelligence Commissioner is responsible for performing quasi-judicial reviews on the issuance of certain authorizations and determinations made by the CSE and pursuant to the Canadian Security Intelligence Service Act. GOVERNMENT OF CANADA, https://www.canada.ca/en/intelligence-commissioner.html (last visited Apr. 13, 2024).

[223] New Zealand's Commissioner of Intelligence Warrants is charged with providing oversight to assure the New Zealand public that the government is acting responsibly and lawfully, including complying with all human rights obligations recognized by New Zealand law. Commissioners must have previously held office as a judge of the High Court and are appointed for three-year terms. Their functions and responsibilities include considering applications for: (i) any warrant that relates to a New Zealander, (ii) practice warrants, which enable the government to carry out activities that are necessary to test, maintain, and develop the capabilities of or train staff, (iii) access to restricted information, and (iv) business records approval, which enable the Director-General of Security to issue business records directions to obtain certain basic information from telecommunications or financial service providers. The office's independence was significantly strengthened in the Intelligence and Security Act of 2017. NEW ZEALAND SECURITY INTELLIGENCE SERVICE, https://www.nzsis.govt.nz/about-us/oversight/ (last visited Apr. 13, 2024).

[224] New Zealand's Office of the Inspector-General of Intelligence and Security was first established in 1996 and became a statutory position through the Intelligence and Security Act of 2017. The Office provides independent oversight of the country's Security Intelligence Service and the Government Communications Security Bureau, which are New Zealand's primary civilian intelligence and security agencies. Its responsibilities include: (i) investigating complaints about the intelligence and security agencies; (ii) conducting inquiries into the activities of the

Commissioner's Office;[225] and the U.S.'s Office of the Inspector General of the Intelligence Community.[226] According to the council's charter, signed in 2017, it was established to provide a forum for council members to:

> exchange views on subjects of mutual interest and concern; compare best practices in review and oversight methodology; explore areas where cooperation on reviews and the sharing of results is permitted where appropriate; encourage transparency to the largest extent possible to enhance public trust; and maintain contact with political offices, oversight and review committees, and non-Five Eyes countries as appropriate.[227]

The IC IG's role with this collaborative partner yields insights capable of resolving the concern about the lack of input from foreign partners. Indeed, the FIORC may present a place to build consensus and common practices on vulnerability use, disclosure, and information sharing. As more countries publish their disclosure decision or equities processes, scholars and others will be able to conduct comparative analyses and more nuanced critiques. The

---

intelligence and security agencies; (iii) reviewing all warrants and authorizations issued to the intelligence and security agencies; (iv) reviewing the intelligence and security agencies' compliance procedures and systems, and (v) receiving protected disclosures relating to classified information or the activities of the intelligence and security agencies. Notably, the office does not have oversight of the following government entities: intelligence branches of the armed services; the intelligence units of the Police, Customs, and the Ministry of Primary Industries and Immigration New Zealand; or the intelligence reporting and policy units of the Department of the Prime Minister and Cabinet. Importantly, the Office of the Inspector-General is an independent entity, and not part of either the Security Intelligence Service or the Communications Security Bureau. INSPECTOR-GENERAL OF INTELLIGENCE AND SECURITY, https://igis.govt.nz/ (last visited Apr. 12, 2024) (emphasizing that an effective intelligence oversight system includes at least one civilian institution that is independent of both the intelligence services and the executive).

[225] The United Kingdom's Investigatory Powers Commissioner's Office (IPCO) was established in 2017 as the result of a merger of three precursor organizations. The IPCO independently oversees the use of the government's investigatory powers, ensuring they are in accordance with the law and in the public interest. The IPCO oversees the use of covert investigatory powers by more than 600 public authorities, including the U.K.'s intelligence agencies, law enforcement agencies, police, councils, and prisons. The IPCO also independently reviews applications from public authorities to use the most intrusive powers and check that all the powers are in accordance with the law. Most notable for our purposes, the IPCO oversees the use of statutory powers by the Government Communications Headquarters (GCHQ) which participates in the disclosure of vulnerability equities and the National Cyber Security Centre (NCSC) which conducts vulnerability research. INVESTIGATORY POWERS COMMISSIONER'S OFFICE, https://www.ipco.org.uk/ (last visited Apr. 12, 2024).

[226] OFFICE OF THE INTELLIGENCE COMMUNITY INSPECTOR GENERAL, https://www.dni.gov/index.php/who-we-are/organizations/icig/icig-who-we-are (last visited Apr. 12, 2024).

[227] FIORC CHARTER, *supra* note 219, ¶ 2.

comparisons may have the added benefit of encouraging countries to recalibrate their policies to ensure consistency, continued cooperation with international partners, and the development of norms of responsible behavior in cyberspace. The FIORC also provides a forum for consideration of developments on the international stage aimed at regulating the use of commercial spyware by governments.[228]

A final point on partnership derives from the IG's ability to conduct oversight work across government agencies and the IC IG's collaborative relationships with other key players in the oversight ecosystem. These partners include entities outside the executive branch, such as the Government Accountability Officer (GAO); entities within the executive branch including the Privacy and Civil Liberties Oversight Board (PCLOB), the President's Intelligence Advisory Board, and the recently established Data Protection Review Court; and entities within the Intelligence Community including the Office of General Counsel to the Director of National Intelligence, and the Office of Civil Liberties, Privacy, and Transparency.[229]

C. Reform Priorities

With an understanding of the IC IG's unique attributes, let's turn now to consider how those attributes can be utilized to accomplish the task of right-setting the oversight lens for the government's use of vulnerabilities. Four areas should be prioritized in efforts to reform the U.S. VEP and the government's use of vulnerabilities. First, it is time to formalize the policy as an executive order. The U.S. VEP, as described by Rob Knake, currently exists only as "an

---

[228] *See* Lubin, *supra* note 12, at 13–17 (summarizing efforts by international actors including the Wassenaar Arrangement, Export Controls, and Human Rights Initiative, and recently adopted Code of Conduct for Enhancing Export Controls of Goods and Technology That Could be Misused and Lead to Serious Violations or Abuses of Human Rights); *see also supra* notes 104–06 and accompanying text (describing the Pall Mall Process and other international developments).

[229] *See* JOHNSON & NEWCOMER, *supra* note 173, at 152–59 (describing IGs interactions and partnerships with other oversight entities and mechanisms); GOLDSMITH, *supra* note 170, at 207 (using term "presidential synopticon" to describe a group of watchers, inside and outside the government, able to check executive branch power and hold executive branch actors accountable); Adam Klein, *National Security Surveillance in the United States: Laws, Institution, and Safeguards*, STRAUSS CTR. FOR INT'L SEC. & L. 10–14 (2024) (describing oversight entities). While the IC IG is not an exclusive answer to the vulnerability oversight challenge, its partnerships with other oversight entities amplify and strengthen its contributions and guidance through the wider oversight framework.

agreement among agencies."[230] Calls to elevate its status to an executive order should be heeded. This will lend formality while maintaining flexibility and discretion. Calls for codification of the U.S. VEP in the U.S. Code are well-intentioned but unlikely to address concerns about lack of transparency and potential abuse. Indeed, such calls may run headlong into Congress's well-documented lack of technical understanding, and may instead result in stale, ineffective constraints that do not accurately reflect the technical environment or the vulnerabilities market. Due to the need for secrecy and responsiveness in cyber operations, this area is better left to executive branch discretion, allowing for nimble revision where needed, and as supplemented by congressional reporting and robust internal oversight.

Structural changes to the U.S. VEP should be a second priority, and these changes should focus on administrative leadership and process. If a leadership change has not already occurred, the home agency for the Executive Secretariat should be reassigned from the National Security Agency (NSA) to the Office of the National Cyber Director (ONCD).[231] Moving the Executive Secretariat to a civilian agency tasked with private sector collaboration will counter the perception that the U.S. VEP tilts in favor of national security equities and will demonstrate that the revised VEP appropriately incorporates industry and privacy perspectives.

A third reform priority should focus on adding new players and their perspectives to the U.S. VEP balancing process. Reforms should create a channel for industry input on decisions by the ERB, either by adding industry representatives to the board or providing a mechanism for industry input during the assessment process. While the ERB currently includes representatives from the Departments of Commerce and Energy, their

---

[230] Robert Knake, *Grading the New Vulnerabilities Equities Policy: Pass*, COUNCIL ON FOREIGN RELS. BLOG (Nov. 17, 2017), https://www.cfr.org/blog/grading-new-vulnerabilities-equities-policy-pass.

[231] The establishment (and in some cases re-establishment) of key cyber positions in the executive branch during the Biden administration lend momentum to calls for reassignment of the Executive Secretariat. These include the appointment of a deputy national security advisor for cyber and emerging technology to the National Security Council, a National Cyber Director, and a Director of the Cybersecurity and Infrastructure Security Agency at the Department of Homeland Security. These are welcome developments after the former administration eliminated the cybersecurity coordinator position in 2018. While questions remain about each position's ability to affect meaningful change and the relationship between the positions, all three are likely to participate in the equities review process in some manner and to be tasked with considering reforms to the VEP. Andrew Grotto, *How to Make the National Cyber Director Position Work,* LAWFARE (Jan. 15, 2021), https://www.lawfaremedia.org/article/how-make-national-cyber-director-position-work; Joshua Rovner, *A Lower Bar for the Cyber Czar*, WAR ON THE ROCKS (Jan. 26, 2021), https://warontherocks.com/2021/01/a-lower-bar-for-the-cyber-czar/.

presence has not proven adequate to the task of protecting private sector interests. As shown in Ashely Deeks' work on "secrecy surrogates," the inclusion of private sector representatives in classified national security decision-making bodies offers significant benefits.[232] These representatives provide technical expertise and also serve as external checks on abuses of governmental secrecy.[233] A related reform in the new player category is the creation of a channel for input from the international community and particularly foreign partners. Prioritizing the structural reforms noted above will align the U.S. government's legitimate use of vulnerabilities with its efforts to achieve private-sector collaboration and with its goal of strengthening norms of responsible state behavior in cyberspace.

The fourth priority for reform should focus on expanding and strengthening oversight and transparency mechanisms by tasking the IC IG with VEP-specific reporting responsibilities. The common call among those who study vulnerability disclosure process and those who have assessed the U.S. VEP's strengths and flaws is for increased transparency and oversight by an independent entity. "Transparency reporting should be done annually and in a manner that enables outside experts to assess whether on balance, the vulnerability assessment and management process is increasing the overall security of the internet ecosystem by prioritizing disclosure and permitting well-justified instances of vulnerability retention."[234] The congressional reporting structure, codified at 50 U.S.C. 3316a, is an admirable first effort at external oversight and transparency. It will benefit, however, from calls for clarification and expansion. As explored in the section below, a key component in accomplishing these reforms is to shift some of the oversight responsibility to the IC IG and to augment the IG's toolkit where needed.

D. Auditing the Vulnerability Stockpile

This next section considers what IC IG oversight might look like in the vulnerability context. Through the use of performance audits and its collaborative partners, the IC IG can contribute to the vulnerability oversight

---

[232] Deeks, *Secrecy Surrogates*, *supra* note 122, at 1438–42.

[233] Smith, *supra* note 2; Dixon, *supra* note 21.

[234] HERPIG, WEIGHING, *supra* note 22, at 27; *see also Pall Mall Process*, *supra* note 7, at paragraph 11.3 (identifying oversight as a critical pillar); *Guiding Principles on Government Use of Surveillance Technologies*, U.S. DEP'T OF STATE 3 (Mar. 30, 2023), https://www.state.gov/guiding-principles-on-government-use-of-surveillance-technologies/ (identifying oversight and accountability and transparency as key principles); CEPS, VULNERABILITY DISCLOSURE IN EUROPE, *supra* note 26, at ix (identifying "independent oversight and transparency" including "[r]egular public reporting" as desirable characteristics of government vulnerability disclosure processes).

ecosystem in a variety of ways, from assessing compliance with the current reporting requirements to evaluating how the government handles deconfliction to recommending programmatic changes. The four examples described below are by no means exhaustive; rather, they are provided to give a sense of the analytic heft and guidance that can be harnessed by involving the IC IG in the oversight work.

An initial and simple IG effort would be a review that assessed whether the DNI was complying with the current congressional reporting requirements.[235] The scope of the review would be to determine whether the required reports were being submitted to the relevant committees in a timely manner. And if so, why was there a delay in publishing the unclassified annex? If not, what was the cause, reason, or factor responsible for the current failure to comply? Does the bottleneck reside in the VEP's Executive Secretariat, with the DNI, or some other actor? While seemingly easy and arguably unnecessary, this initial review would answer the question "where are the reports?" and start to tackle some of the transparency and accountability critiques.

A second review could involve a relatively straightforward information-gathering exercise. It would address the critique that the current reporting requirements are feeble and limited and provide a granular review of the number of vulnerabilities being touched by (or excluded from) the U.S. VEP's review process in the past three to five years. The more detailed, year-to-year, information would aid key policymakers, including the DNI and relevant congressional committees, to assess the accuracy of the critiques described above. It may be particularly helpful in assessing the effects stemming from the lack of industry and privacy perspectives and the size of the purchasing loophole. Congress could statutorily mandate such a report, or the DNI could task the IC IG with this work, or the IC IG could identify this as an area in need of review on their own.[236] The table below provides a starting point for the review:

---

[235] The charter requires reporting to Congress, and publication of an unclassified annex. U.S. VEP, *supra* note 9, at Section 4.3. The statutory requirements include similar reporting mandates. 50 U.S.C. § 3061a. Yet these reports are not readily available to the public, leading many to wonder if the reporting is even occurring. A compliance review would provide some answers. The IC IG should be tasked with conducting a review that assess whether the statutorily-required reports are being submitted to the relevant congressional committees.

[236] *See, e.g.*, PATCH Act, *supra* note 107, and other legislative efforts tasking the DHS IG or IC IG with preparing and submitting such reports. *See also* 50 U.S.C. § 3033(b)(1) ("purpose of the Office of the Inspector General of the Intelligence Community is. . . to create an objective and effective office, appropriately accountable to Congress, to initiate and conduct independent investigations, inspections, audits, and reviews on programs and activities"); WILHELM, *supra* note 173, at 7; JOHNSON & NEWCOMER, *supra* note 173, at 96–97, 132–35.

Table: Review of Vulnerabilities Submissions to the U.S. VEP

For the calendar year indicated, provide:	**CY 2023**	**CY 2022**	**CY 2021**
the number of vulnerabilities submitted for initial review (exclude reassessments of previously restricted or retained vulnerabilities)			
the number of vulnerabilities submitted for initial review, organized by submitting entity (NSA, FBI, etc.)			
of the vulnerabilities submitted for initial review, the number of vulnerabilities disclosed to a vendor or the public			
of the vulnerabilities disclosed to a vendor or the public as a result of the VEP process, the number known to have been patched (and any related information on the time from disclosure to patch)			
of the vulnerabilities submitted for initial review, the number of vulnerabilities retained, and then organized by anticipated use and/or reason for retention (i.e., law enforcement, intelligence collection, etc.)			
the aggregate number of the vulnerabilities excluded from review under VEP paragraph 5.4, organized by exclusion category (e.g., non-disclosure agreement, sensitive operation, foreign partner request, research, etc.) and			

organized by entity			
the number of previously retained vulnerabilities that were reassessed pursuant to VEP section 5.2.5			
of the number of reassessed vulnerabilities, the number of initial determinations that were changed (i.e., from restrict to disclose, etc.)			
the number of ERB meetings (and the entities present at each meeting)			
of the vulnerabilities submitted for initial review, the number of ERB determinations reached by consensus (no challenge)			
of the vulnerabilities submitted for initial review, the number of ERB determinations subject to challenges, organized by challenging entity			

The table above is designed to provide a sample or template for members of Congress, congressional staff, agency office holders, or employees of inspector general offices. Its goal is to offer one mechanism for addressing the transparency and accountability concerns surrounding the use of vulnerabilities and the vigor of the U.S. VEP. As noted above, these concerns persist as there is little evidence that the intra- and inter-branch reporting requirements are being met. Presumably, the report for this review would be classified. However, it may be possible to create an unclassified version of this report which could be included in the Annual Statistical Transparency Report Regarding the Use of National Security Authorities, prepared by the Office of the Director of National Intelligence.[237]

A third example would be to task the IC IG with conducting an evaluation that compares agency interpretations and processes for identifying vulnerabilities that meet the U.S. VEP's threshold requirements for submission. The review would be designed to address the inconsistency and exclusions

[237] OFF. OF THE DIR. OF NAT'L INTEL., ANN. STAT. TRANSPARENCY REP. REGARDING THE INTEL. CMTY.'S USE OF NAT'L SEC. SURVEILLANCE AUTHORITIES FOR CALENDAR YEAR 2022 (2023).

critiques. The scope of the work would build on the categories in the congressionally mandated reports and possibly add follow-on questions, such as:

- Which officials in the agency are responsible for determining whether a vulnerability should be submitted for review?
- What type of training do those officials receive?
- What process does the agency use to make that determination?
- Is the process documented or logged?
- What criteria does the agency use to make that determination?
- Has there been a "significant change" in the process?
- Has there been any other revisions to the process not rising to the level of significant change?
- Does the agency conduct a post-hoc review process after the ERB determination process?
- How does your agency define "sensitive operation" for purposes of the exceptions section?

The IC IG Forum would be an ideal starting point for discussions on how to set the parameters of the review and how to develop an audit team with the necessary technical expertise and knowledge of the participating entities. This review may have both audit and evaluation components, leading to a final report that provides important insights as to gaps, inconsistencies, and areas of conflict. In addition, the review may offer a mechanism for considering whether and how the U.S. VEP is in alignment with the national cybersecurity strategy and other vulnerability disclosure efforts and mandates.[238] The IC IG Forum is particularly well-equipped to address inconsistent interpretations. If appropriate, based on the information gathered during the review, the IC IG should recommend corrective action for harmonizing the different approaches, including whether additional guardrails are needed on aspects of the vulnerability retain/disclose decision-making process.[239]

A final example would be an audit that gathers expenditure data, organized by agency, on the purchasing of vulnerabilities by the U.S. government. The timing may be optimal for a review of the U.S. VEP's vulnerability purchasing exception as recent reporting mandates on commercial spyware are coming

[238] *See supra* notes 63–75 and accompanying text in Section I (describing executive and legislative authorities enacted since the publication of the U.S. VEP charter in 2017).

[239] The ability to issue not only findings but also recommendations based on those findings allows IGs to offer "broad proposals for change." LIGHT, *supra* note 170, at 19.

due.[240] The two areas are closely intertwined: "What is the point of having an equities process if a country can simply sidestep it by buying commercial spyware from a foreign vendor?"[241] Such information will help Congress assess whether the purchasing loophole is swallowing the policy's goal of balancing the government's needs with public and private sector interests.

CONCLUSION

The WannaCry and NotPetya attacks revealed the "friendly fire" challenges that accompany the use of vulnerabilities by government entities, even when the intended purpose constitutes a legitimate intelligence collection or defense objective. While there is little doubt that vulnerabilities are part and parcel of any state's national security toolkit, the potential for unintended and far-reaching effects counsels for robust accountability and oversight mechanisms. The challenge is to find an oversight mechanism or player matched to the needs of the capability and the potential for abuse. When published in 2017, the U.S. VEP was touted as such a mechanism. Its stated purpose was to prioritize the public's interest "through the disclosure of vulnerabilities discovered by the USG, absent a demonstrable, overriding interest in the use of the vulnerability for lawful intelligence, law enforcement, or national security purposes."[242] The U.S. VEP, however, has proved to be a flawed mechanism, one that must be reformed in a manner that appropriately calibrates the governmental, industry, foreign partner, and privacy interests at stake in vulnerability-related decisions. The IC IG is an essential component in that recalibration.

The IC IG brings a set of tools and capabilities well-matched to the task of ensuring the government's use of vulnerabilities complies with the relevant legal and policy authorities, incorporates privacy and civil liberty considerations, and is consistent with shared goals of industry and foreign partners. In the course of conducting performance audits and inspections, the IC IG and its partners are able to flag concerning operational and deconfliction issues, identify interpretative discrepancies, and direct policymakers—Congress and agency heads—to those areas in need of urgent attention and reform. Prioritizing the reforms noted above and giving this often overlooked player a more significant role in the oversight ecosystem will align the government's use of vulnerabilities for legitimate intelligence, law enforcement, and defense

---

[240] *See supra* notes 66 & 70 and accompanying text in Section I (describing commercial spyware vendor reporting requirements in NDAA FY2023).
[241] Lubin, *supra* note 12, at 28.
[242] U.S. VEP, *supra* note 9, at Section 1.

purposes with efforts to ensure the protection of privacy interests and achieve effective private-sector collaboration while aligning the government's conduct with evolving norms of responsible behavior in cyberspace.