9-2-2021

It's Time to Reform the U.S. Vulnerabilities Equities Process

Amy Gaudion
Penn State Dickinson Law, acg14@psu.edu

IT’S TIME TO REFORM THE U.S. VULNERABILITIES EQUITIES PROCESS

warroom.armywarcollege.edu/articles/vep/

By Amy Gaudion

> Since its inception, scholars, journalists, and former government officials have warned of the VEP’s limitations, loopholes, and the need for oversight.

In May of 2017, the WannaCry attack, later attributed to North Korea and Russia respectively, resulted in the loss of billions of dollars for governments and private companies across the globe. A month later, the NotPetya attack, later attributed to Russia, wreaked additional and more devastating havoc, again on a global scale. Both attacks exploited a vulnerability found in the Microsoft Windows operating system. The United States government had discovered the same vulnerability many years earlier. Rather than notifying Microsoft of the vulnerability so that it could be patched, the United States government decided to keep the vulnerability secret so that it could be utilized for national security and intelligence purposes. In assessing whether to disclose or retain the vulnerability that led to the WannaCry and NotPetya attacks, the United States government followed an internal executive branch policy called the Vulnerabilities Equities Policy and Process, more commonly known as the VEP.

The VEP guides the decision-making process when the United States government discovers exploitable weaknesses, or vulnerabilities, in information systems. It is the process by which the government decides whether to disclose the security flaws it discovers or to keep the

flaws secret for national security, intelligence, or law enforcement purposes. According to the charter, the VEP provides an interagency mechanism that seeks to balance "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, and potentially other partners, so that it can be used for national security and law enforcement purposes, such as intelligence collection, military operations, and/or counterintelligence." Since its inception, scholars, journalists, and former government officials have warned of the VEP's limitations, loopholes, and the need for oversight. Despite these warnings, the VEP has remained a policy in the shadows. A confluence of recent events, however, has created a window of opportunity for substantive review and meaningful reform of this little-known but consequential policy.

The first condition favoring reform is provided by the fallout from the Kaseya, Colonial Pipeline, SolarWinds and Microsoft Exchange attacks. They provide compelling reminders that government and private sector networks are intimately connected and inter-dependent, and that the need for timely and accurate information sharing is critical. This observation, while obvious, requires constant repetition as the United States government continues to embrace policies that segment public and private sector responsibility for cybersecurity. The much-heralded Cyberspace Solarium Commission Report highlighted the need to "operationalize cybersecurity collaboration with the private sector." The report urged the United States government and industry to develop "a new social contract of shared responsibility to secure the nation in cyberspace." The new arrangement must include better information sharing mechanisms to achieve "truly shared situational awareness" of cyber threats. To do so, the information flows must run both ways, from industry to the government and from government to industry. The VEP is often criticized for blocking the government to industry flow, and for creating distrust in its wake. As each day brings new developments on the scope of the SolarWinds and Microsoft Exchange breaches, calls to reform the VEP are resonating with occupants of the White House and Capitol Hill.

The second condition creating support for VEP reform is the establishment (and in some cases re-establishment) of key cyber positions in the executive branch. President Biden appointed Anne Neuberger to the post of deputy national security advisor for cyber and emerging technology on the National Security Council, Chris Inglis as the National Cyber Director, a position created by Congress in the most recent defense authorization act, and Jen Easterly as the 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. All three are likely to participate in the equities review process in some manner, and to be tasked with considering reforms to the VEP. While questions remain about each position's ability to affect meaningful change and the relationship between the positions, their formation prepares the architecture needed to adopt a whole of government approach to cyber threats and responds to calls for

a new national cyber strategy. A reassessment of the VEP's role and effectiveness will certainly be a component of the larger cyber strategy review project.

A third condition favoring VEP reform is the trend toward publication of equities processes by other nations. Several allies have recently done so. The UK published its Equities Process in November 2018, followed by Australia's Responsible Release Principles for Cyber Security Vulnerabilities in 2019. The demand for public commitments by nations is coming from companies and think tanks, including reports from the Centre for European Policy Studies (CEPS), Transatlantic Cyber Forum, and Carnegie Endowment for International Peace. These calls include demands to identify the entities involved in the vulnerability assessment process, to add private sector representation, to agree on assessment standards, to shorten retention times, and to shorten the time between reassessments of retained vulnerabilities. As more countries publish their equities processes, creating opportunities for comparative analysis and critique, the United States will have to recalibrate its VEP to ensure consistency and continued cooperation with its international partners.

These conditions set the stage for reconsideration of the VEP and create an environment where failure to contemplate reforms will be condemned, appropriately so, by critics in the United States as well as the international community. A full review of recommended changes is beyond this essay's scope, however, four items should be priorities in any reform effort. First, it is time to formalize the policy as an executive order. The VEP, as described by Rob Knake, currently exists only as "an agreement among agencies." Calls to elevate its status to an executive order should be heeded. Doing so will lend formality while maintaining flexibility and discretion. Calls for codification of the VEP in the United States Code are well-intentioned but unlikely to address concerns about lack of transparency and potential abuse. Codification 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 balanced by effective congressional reporting and internal oversight mechanisms.

> While NSA is well-staffed and resourced to serve as the 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 of the vulnerability for national security or intelligence collection purposes.

Structural changes to the VEP should be a second priority, and should include reassignment of the Executive Secretariat from the National Security Agency (NSA) to the Cybersecurity and Infrastructure Security Agency (CISA) within the Department of Homeland Security (with a possible future transfer to office of the national cyber director once established). As noted by Sven Herpig, "institutional setup is one of the toughest challenges in designing" equities processes. Selection of the lead agency should be placed with an entity able to balance the

competing equities and avoid unduly favoring the national security interests. While NSA is well-staffed and resourced to serve as the 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 of the vulnerability for national security or intelligence collection purposes. The trust deficit was badly damaged by NSA's decision to retain the EternalBlue vulnerability until 2017. Despite NSA's recent efforts to rebuild trust with private sector partners, the residue of that retention casts a long shadow. Moving the Executive Secretariat to a civilian agency tasked with private sector collaboration will counter the perception that the VEP tilts in favor of national security equities, and will demonstrate that the revised VEP appropriately incorporates industry perspectives.

A third reform priority, also focused on the VEP's structure, should create a channel for private sector input on decisions by the Equities Review Board (ERB), either by adding industry representatives, 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 presence has not proven adequate to the task of protecting private sector interests. As shown in Ashely Deeks' recent work on "secrecy surrogates", the inclusion of private sector representatives in classified national security decision-making bodies offers significant benefits. These representatives provide technical expertise and also serve as external checks on abuses of governmental secrecy. Prioritizing the structural reforms noted above will align the United States government's use of vulnerabilities for legitimate intelligence, law enforcement, and defense purposes with its efforts to achieve private-sector collaboration.

The fourth priority for reform should focus on strengthening oversight and transparency mechanisms. 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. The annual report's content should be expanded to include the number of vulnerabilities retained, the specific purpose for retention, the length of retention, as well as information on the retention reassessment process. It also should include more granular information about the vulnerabilities excluded under Section 5.4 of the VEP. The revised reporting requirements should highlight decisions to retain due to non-disclosure agreements or memoranda of understanding with foreign and research partners. For example, the report should include information on the number and cost of vulnerabilities purchased by each agency. This information will help Congress assess whether the purchasing exception, which by one estimate calculated the NSA's 2013 budget for zero-day vulnerability purchases at $25.1 million, is swallowing the policy's goal of balancing the government's need with public and private sector interests. In addition, the committee recipients of the classified annual report should be expanded beyond the intelligence committees to also include the defense committees in the House and Senate. Indeed, the chairs of the newly established Subcommittee on Cyber, Innovative Technologies, and

Information Systems (CITI), are likely to be interested in such. Finally, while the statute requires an "unclassified appendix," that document is not readily available to the public. Reforms should heed prior calls for the issuance of public annual reports.

Related reforms are needed regarding internal oversight. A prior legislative proposal called for the Inspector General of the Intelligence Community (IG IC) to conduct an annual audit of VEP decisions. Congress should revisit this proposal and task the IG IC (or preferably the IG of DHS) with the annual audit task and an audit of each agency's internal VEP process. This will ensure consistency in the way vulnerabilities are selected for – or excluded from – submission to the VEP. These oversight reforms will improve transparency in the VEP while not unduly hampering the executive branch's need for flexibility in the use of vulnerabilities to support offensive and defensive cyber measures. The VEP's stated purpose is to "prioritize the public's interest in cybersecurity and to protect 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 for lawful intelligence, law enforcement, or national security purposes." There is no doubt the VEP serves a critical function in a time when cyber capabilities are essential to national defense. It must, however, be pulled from the shadows to effectively serve that function, and reformed in a manner that appropriately calibrates the interests at stake. The conditions are right for reform of the VEP, and the priorities offered above will clarify how and when the United States government may utilize vulnerabilities while also establishing the United States as a leader of responsible behavior in cyberspace.

Amy C. Gaudion *is the associate dean for academic affairs and professor of lawyering skills at Penn State Dickinson Law. Her teaching and scholarship focus on national security law, cyberspace law and policy, and civilian-military relations.*

The views expressed in this article are those of the author and do not necessarily reflect those of the U.S. Army War College, the U.S. Army, or the Department of Defense.

Photo Credit: Background vector created by rawpixel.com – www.freepik.com