Improving and Making the Vulnerability Equities Process Transparent is the Right Thing to Do

NOVEMBER 15, 2017 AT 9:11 AM ET BY ROB JOYCE

There can be no doubt that America faces significant risk to our national security and public safety from cyber threats. During the past 25 years, we have moved much of what we value to a digital format and stored it in Internet-connected devices that are vulnerable to exploitation. This risk is increasing as our dependence on technology and the data we store continues to grow such that technology now connects nearly every facet of our society and the critical services that sustain our way of life. This fact is not lost on criminal actors and adversarial nation states who discover and exploit existing flaws in software, hardware, and the actions of legitimate users to steal, disrupt, and destroy data and services critical to our way of life.

Just as people expect government to defend the physical world, they also expect government to pursue criminals and other rogue actors in the cyber world and hold them accountable, both to punish bad acts and to deter future misbehavior. At the same time, governments must promote resilience in the digital systems architecture to reduce the possibility that rogue actors will succeed in future cyber attacks. This dual charge to governments requires them to sustain the means to hold even the most capable actor at risk by being able to discover, attribute, and disrupt their actions on the one hand, while contributing to the creation of a more resilient and robust digital infrastructure on the other. Obtaining and maintaining the necessary cyber capabilities to protect the nation creates a tension between the government's need to sustain the means to pursue rogue actors in cyberspace through the use of cyber exploits, and its obligation to share its knowledge of flaws in software and hardware with responsible parties who can ensure digital infrastructure is upgraded and made stronger in the face of growing cyber threats.

Our national capacity to find and hold criminals and other rogue actors accountable relies on cyber capabilities enabled by exploiting vulnerabilities in the digital infrastructure they use. Those exploits produce intelligence for attribution, evidence of a crimes, enable defensive investigations, and posture us to respond to our adversaries with cyber capabilities. The challenge is to find and sustain the capability to hold rogue cyber actors at risk without increasing the likelihood that known vulnerabilities will be exploited to harm legitimate, law-abiding users of cyberspace. This is the root of the tension that exists between the desire to publicize every vulnerability discovered by the Federal Government in the conduct of its law enforcement and national security responsibilities and the need to preserve some select capability for action against extremely capable actors whose actions might otherwise go undiscovered and unchecked.

In recognition of these competing considerations, newly-discovered cyber vulnerabilities that are not yet in the public domain are submitted into an interagency process known as the Vulnerabilities Equities Process (VEP). At its most basic level, the VEP is charged with balancing whether to disclose vulnerability information to the vendor with expectation that they will patch the vulnerability, or temporarily restrict knowledge of the vulnerability so that it can be used for national security or law enforcement purposes. I believe that conducting this risk/benefit analysis is a vital responsibility of the Federal Government

The United States is a world leader when it comes to sophisticated processes and conversation on this topic, and no other nation in has created and run a process as advanced, meticulous, and transparent as ours. While not infallible, these processes ensure rigorous consideration of all factors vital to our national security. The Federal Government also has an important responsibility to closely guard and protect vulnerabilities as carefully as our military services protect the traditional weapons retained to fight our nation's wars.

Unauthorized disclosures undermine public confidence and damage our ability to carry out intelligence missions. Recent cybersecurity incidents of global impact have heightened our interest and awareness in ensuring we conduct the VEP in a manner that can withstand a high degree of scrutiny and oversight from the citizens it serves.

I believe that conducting this risk/benefit analysis is a vital responsibility of the Federal Government. There are advocates on both sides of the vulnerability equity issue who make impassioned arguments. Some argue that every vulnerability should be immediately disclosed to the vendor and patched. In my view, this is tantamount to unilateral disarmament. Our adversaries, both criminal and nation state, are unencumbered by concerns about transparency and responsible disclosure and will certainly not end their own programs to discover and exploit vulnerabilities.

Further, the lack of visibility into the discovery efforts of our adversaries makes it unlikely that Federal Government disclosures will close the same holes they exploit. At the opposite extreme are those who believe that intelligence collection and operations for national security should be prioritized over network defense concerns and this is a belief held by many nations.

Although I don't believe withholding all vulnerabilities for operations is a responsible position, we see many nations choose it. I also know of no nation that has chosen to disclose every vulnerability it discovers.

In considering a way forward, there are some key tenets on which we can build a better process.

Improved transparency is critical. The American people should have confidence in the integrity of the process that underpins decision making about discovered vulnerabilities. Since I took my post as Cybersecurity Coordinator, improving the VEP and ensuring its transparency have been key priorities, and we have spent the last few months reviewing our existing policy in order to improve the process and make key details about the VEP available to the public. Through these efforts, we have validated much of the existing process and ensured a rigorous standard that considers many potential equities.

The interests of all stakeholders must be fairly represented. At a high level we consider four major groups of equities: defensive equities; intelligence / law enforcement / operational equities; commercial equities; and international partnership equities. Additionally, ordinary people want to know the systems they use are resilient, safe, and sound. These core considerations, which have been incorporated into the VEP Charter, help to standardize the process by which decision makers weigh the benefit to national security and the national interest when deciding whether to disclose or restrict knowledge of a vulnerability.

Accountability of the process and those who operate it is important to establish confidence in those served by it. Our public release of the unclassified portions Charter will shed light on aspects of the VEP that were previously shielded from public review, including who participates in the VEP's governing body, known as the Equities Review Board. We make it clear that departments and agencies with protective missions participate in VEP discussions, as well as other departments and agencies that have broader equities, like the Department of State and the Department of Commerce. We also clarify what categories of vulnerabilities are submitted to the process and ensure that any decision not to disclose a vulnerability will be reevaluated regularly. There are still important reasons to keep many of the specific vulnerabilities evaluated in the process classified, but we will release an annual report that provides metrics about the process to further inform the public about the VEP and its outcomes.

Our system of government depends on informed and vigorous dialogue to discover and make available the best ideas that our diverse society can generate. This publication of the VEP Charter will likely spark discussion and debate. This discourse is important. I also predict that articles will make breathless claims of "massive stockpiles" of exploits while describing the issue. That simply isn't true. The annual reports and transparency of this effort will reinforce that fact.

The departments and agencies that participated in the creation of the VEP take their responsibility to be transparent with the public while safeguarding sensitive information very seriously, and the equities decisions we have to make are hard. There are rarely black and white answers. The VEP ensures we bring together informed and educated participants on both sides of the issue to make the best possible decisions for the nation.

Vulnerability management requires sophisticated engagement to ensure protection of our people, the safeguarding of critical infrastructure, and the defense of important commercial and national security interests. I believe our newly endorsed VEP Charter helps us balance those interests in a way that is repeatable and defensible. By making it public, we hope to demonstrate to the American people that the Federal Government is carefully weighing the risks and benefits as we carry out this important mission.

You can read the VEP Charter here and the fact sheet here.

Rob Joyce is the White House Cybersecurity Coordinator.