# The four problems with the US government's latest rulebook on security bug disclosures

## But it's still better than nothing

By Kieren McCarthy in San Francisco 15 Nov 2017 at 22:59

**Analysis** The United States government has published its new policy for publicly disclosing vulnerabilities and security holes.

The new rulebook [PDF] – and the decision to make it public – comes following a tumultuous 12 months in which Uncle Sam's chief spy agency, the NSA, was devastated to discover part of its secret cache of hacking tools and exploits had been stolen, were available for sale, and later leaked all over the internet for free.

The shockwaves from that cyber-weapon dump were felt across the world, with hospitals in the UK among organizations knackered by the WannaCry malware, which wielded the leaked NSA exploit code to infect vulnerable Windows computers.

There is no mention in the US government's new "Vulnerabilities Equities Policy and Process" of the dangers of the NSA stockpiling security bugs: when the agency gets its hands on an exploitable vulnerability in a product, it may keep the details private so it can leverage the bug to quietly infect and spy on targets. For example, the aforementioned leaked cyber-weapons exploited one such stockpiled flaw in the Windows network file system code, and thus when the NSA toolkit was leaked online and into the hands of WannaCry's developers, there was no patch available to protect users.

The very existence of the policy document is sufficient proof, though, that the widespread criticism of Uncle Sam's approach to computer security was heard, and acted upon.

The most important part of the new policy is that it states that the default action when the US government discover a new security hole should be to disclose it to the relevant software companies. It states: "In the vast majority of cases, responsibly disclosing a newly discovered vulnerability is clearly in the national interest."

The other good news is that the many arms of the US government have recognized the importance of speed in disclosing vulnerabilities and have written that into their disclosure rules.

If information on a specific vulnerability is released, the policy gives the US government seven days to react – which is extremely quick when you consider the size the administration and the number of departments that need to be consulted: 10, according to the policy.

If someone within the US government discovers a hole, the process for reviewing and disclosing it is also notable swift:

- A one-day notification period after the new "VEP executive secretariat" is informed for all the other departments to be asked to react and respond.
- Five days for the department to respond – and raise any concerns about disclosing the security hole
- Seven days to reach consensus if someone does raise an objection.
- Resolution within a "timely fashion"
- A goal for consensus but if not, a vote before disclosure

That is all surprisingly efficient and pragmatic. But, of course, there are problems. And so far we have spotted four of them.

## 1. There is a massive NDA loophole

The policy notes: "The USG's decision to disclose or restrict vulnerability information could be subject to restrictions by foreign or private sector partners of the USG, such as Non-Disclosure Agreements, Memoranda of Understanding, or

other agreements that constrain USG options for disclosing vulnerability information."

While it is important to note that there may be restrictions, legal and otherwise, on disclosing vulnerabilities, this part of the policy potentially allows organizations seeking to sell technical details on security holes to block disclosure by concocting an NDA.

## 2. There is no rating of risk

Typically software vulnerabilities are rated according to how potentially dangerous they are. Microsoft, for example, has four ratings of severity: low, moderate, important and critical.

This is useful to sysadmins who know whether to focus on a patch immediately or leave it a more convenient time, although it must be said that Microsoft tends to label stuff as important when really anyone else would call it critical – but you get the point. A rating system also allows a broader assessment of what and how many vulnerabilities are being disclosed.

For example, 100 holes with a low severity rating aren't worth as much as a single critical vulnerability because of the added risk and exposure that a critical hole brings with it.

But there is no mention of ratings in the VEP policy. As such, others will have to assess how significant a bug is – which seems like an unnecessary additional delay, especially since there is no way that the US government does not apply its own internal severity rating.

It is going to be hard to assess whether this new policy is actually achieving much without ratings: the NSA could publicly disclose 999 low and medium risk holes, and still keep five critical ones classified.

With ratings, it would be possible to compare what the US government is

revealing with commercial entities – and so gain an approximation for how many zero-day flaws the USG is sitting no. Which is, presumably, why they have avoided ratings.