THE RED BRANCH REPORT

BECAUSE WASHINGTON IS TOO IMPORTANT TO IGNORE

June 2017

OUR VISION

We aim to bring Washington, DC to Silicon Valley.

The large Valley firms have K St. lobbyists, lawyers, and public relations professionals. The small and mid-size start-ups and entrepreneurs have nobody.

We try to fill that gap. This monthly newsletter has "news you can use" that may be important to the IT start-up sector. You may not have the resources to track it, but Washington is too important to ignore.

The US Capitol at dawn

THE PATCH ACT AND THE ACTIVE CYBER DEFENSE CERTAINTY ACT

The non-cyber world certainly seems to be taking up the attention of most of official Washington – so much so that most observers anticipate little, if any, legislative action in the near-term.

That having been said, times like these, where legislation is not under active consideration, are when new ideas get surfaced and developed. Some of them never come to fruition; but for others the seeds of success are planted when trial balloons and legislative policy proposals are floated for consideration. In this issue, we look at two such proposals: The PATCH Act and the Active Cyber Defense Certainty Act.

> *"[T]imes like these, where legislation is not under active consideration, are when new ideas get surfaced and developed."*

The PATCH Act (https://tinyurl.com/ybhfpo3w) was introduced by Representatives Ted Lieu (D-CA) and Blake Farenthold (R-TX) in the wake of the WannaCry ransomware encryption attack. A parallel bill in the Senate was introduced by Brian Schatz (D-HI), Ron Johnson (R-WI) and Cory Gardner (R-CO). The impetus for the bill was a public report that the WannaCry ransomware took advantage of an exploit in the Windows operating system that the US government had known about; had failed to disclose to Microsoft; had been stolen from NSA; and had been released to the world by Shadow Brokers, an anonymous group of hackers who have taken to disclosing information about the NSA.

The idea behind the bill is to codify and strengthen the existing process by which the US government determines whether or not to reveal the exploits it learns about to the vendors who wrote the code. It is clear that the bills' authors intend to create a system that strongly favors disclosure. As Senator Johnson said: "It is essential that government agencies make zero-day vulnerabilities known to vendors whenever possible, and the PATCH Act requires the government to swiftly balance the need to disclose vulnerabilities with other national

security interests while increasing transparency and accountability to maintain public trust in the process." The bill is certain to stir debate as to whether the balance it strikes is the right one – and anybody who writes code for profit should be interested in the discussion.

Meanwhile, Representative Tom Graves (R-GA) has published a discussion draft (https://tinyurl.com/ya5cguwm) of a bill entitled the Active Cyber Defense Certainty Act. The bill is notable, I think, for two facts: First, it appears to be the very first legislative effort to codify and authorize any aspect of "hack back" responses to cyber intrusions. Second, the bill is, in reality, a very modest, and limited effort. It does not seek to permit destructive cyber responses and would legalize only hack backs that are for the purpose of information gathering – in other words techniques within the broad category of "beaconing." Again, anyone victimized by cyber intrusions (which is everyone) will be interested in the progress of this discussion.

Our Prediction: Neither bill will become law this year. But this is precisely the moment when entrepreneurs who are interested in the topics would be wisest to intervene. The early development stages of a policy idea, like the early conceptual stages of a new start-up, are when the intellectual DNA for an idea are developed.

THE CYBER EXECUTIVE ORDER

Meanwhile, all is not completely quiet on the executive front. Just as we went to press last month, President Trump issued a cybersecurity executive order (http://bit.ly/2pp97Qf) that will provide the framework for executive action on cybersecurity, at least in the near-term.

This Order, unlike others issued by President Trump, is reasonably characterized as a continuation of existing policy rather than as a disruptive transformation. Indeed, many observers remarked that it could well have been issued by the Obama Administration.

That, perhaps, is a bit too strong. The Order is particularly notable for its emphasis on the role of the private sector in creating cybersecurity and for its de-emphasis of the role of the Federal government. Perhaps more strikingly, the Order is a temporizing document. It calls for (by my count) 16 separate reports, some of which are not due to be finalized for over a year. Based on those reports, the Order requests six separate action plans or strategies to be development. Two things are readily apparent from this structure:

- First, the true nature of this Administration's ambitions in the cyber domain will not be known until the reports are written; the action plans developed; and the resources allocated; and

DHS CANCELS AGILE METHODS CONTRACT

In a blow for the use of agile methods software development in government services, DHS has, apparently, acknowledged a severe misstep.

Last year, the Department awarded a $1.5 billion contract for small business procurement known as Flexible Agile Support for the Homeland (FLASH). The other day, DHS cancelled the contract.

"The goal of FLASH was to give department components access to innovative methods and industry best practices to acquire agile design and development support services. DHS said in the solicitation it was seeking to develop an acquisition contract that includes the concepts from the U.S. Digital Services Playbook such as user-centered design, dev/ops, automated testing and agile. DHS's Procurement Innovation Lab (PIL) was running FLASH."

The initial award, in November 2016 was protested to GAO. A new award in March 2017 was, again, protested by the losing bidders. Rather than fight, DHS has given up and it is not clear what comes next for agile services. The bottom line seems to be that, once again, government systems fight change.

Jason Miller, FedNews Radio, (https://tinyurl.com/ycjhso8j)

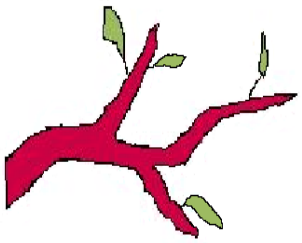
- Second, the Nation's limited storehouse of good cyber talent will, for the next 3-9 months, be spending its time in assessments and report drafting. It is an open question whether sufficient workforce expertise exists to accomplish the assigned tasks in the time specified. It is beyond question that in doing so, the expertise available will be focused on "thinking" rather than on "doing."

In the end, this means that the only reasonable response one can have to the Trump cyber executive order is "wait and see." It may prove to be critical; or it may prove to have been a relatively ineffectual blip. Only time will tell.

WASHINGTON TRACKER

Our regular feature – a tracker for legislation and executive action that might be of interest to Valley entrepreneurs:

Bill # or Agency	Title	Description	Status
FCC	Repeal of Net Neutrality Regulations	The FCC has begun the process of considering how to repeal and/or replace the "net neutrality" regulations adopted by the Commission during the Obama Administraiton. The revised regulations would permit internet providers to charge variable fees to subscribers based on volume and other factors.	With the change in Administration, the revised regulations are very likely to be adopted by the Commission sometime before the end of this year. Expect the revision to be immediately challenged in Federal court, where the outcome is indefinite.
H.R. 2841 S. 1157	PATCH Act	Creates Vulnerabilities Equities Review Board to review decision on disclosure of vulnerabilities discovered by USG agencies to vendors.	Introduced May 17 in House and Senate and referred to committees; hearings may occur this year; passage unlikely.
H.R. 387	Email Privacy Act	Amends the Electronic Communications Privacy Act to require a warrant for government access to cloud-stored emails and other electronic content.	Passed Feb. 6 by voice vote in House; awaiting Senate action. Last Congress bill was killed in Senate; possible same result in 115th Congress.
H.R. 1530	Financial Transparency Act	Significant open data initiative that would direct the government's eight financial regulatory agencies to adopt data standards for the information they collect from the private sector in order to reduce duplication, burden and fraud and make it available for download, accessible via application programming interfaces and easily searchable.	Introduced in House; hoped for introduction of Senate version ahead; in last Congress initiative languished but this has better prospects as OMB Director Mulvaney may be supportive
S. 770	MAIN STREET Cybersecurity Act	Would require NIST to take into account needs of small businesses in setting NIST cybersecurity framework standards.	Introduced in Senate March 29 with bipartisan support. Unlikely to pass independently; may get added to larger bill.
H.R. 1899 S. 823	Protecting Data at the Border Act	Would require border agents to get a search warrant before searching digital devices at the border; currently no warrant is required.	Introduced in House and Senate on April 4; referred to committee; passage unlikely at this time.



Contact Us

Red Branch Consulting, PLLC
Paul Rosenzweig, Esq.
509 Ct. NE
Washington, DC 20002
O: +1 (202) 547-0660
M: +1 (202) 329-9650
VOIP: +1 (202) 738-1739
@RosenzweigP
www.lawfareblog.com
www.redbranchconsulting.com
www.paulrosenzweigesq.com

To subscribe or unsubscribe, send an email to: paul.rosenzweig@redbranchconsulting.com

RECOMMENDED READINGS

The Holder Report on Uber, https://tinyurl.com/y6vo2my9. A cautionary tale about how culture and leadership are critical components of any company, and how failures can affect the bottom line.

THE LAST WORD

"The security of the Internet of Things is an issue of national security." – Melissa Hathaway (former Senior Director for Cybersecurity Policy under President Obama), June 1, 2017, speaking to the American Bar Association Standing Committee on Law and National Security.

If we take Ms. Hathaway seriously (and we should), expect far greater attention to the security of consumer devices. Potential government responses may range from regulation to the impostion of liablity for inadequate security measures.