WASHINGTON
LEGISLATIVE OFFICE

May 27, 2015

Internet Policy Task Force
National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue NW, Room 4725
Washington, DC 20230

Re: Docket Number 150312253-5253-01, Cybersecurity Best Practices

Dear Members of the Internet Policy Task Force,

The American Civil Liberties Union thanks the Internet Policy Task Force for seeking public comment on cybersecurity best practices that can substantially improve security for organizations and consumers.[1] Far too many of the cybersecurity legislative proposals discussed in Washington during the past few years negatively impact civil liberties by expanding the government's surveillance powers.[2] We appreciate the opportunity to present these recommendations on the question of how best to improve the process of computer security vulnerability disclosure, which, if widely implemented, would significantly improve cybersecurity without harming Americans' civil liberties.

All computer systems have programming flaws and design mistakes that can be exploited. Although it is certainly possible to reduce the number of these flaws and their impact, no system will ever be one hundred percent secure. The flaws that do exist may be discovered by researchers—including academics, professionals, and hobbyists working in their spare time— many of whom will try to report the flaws to the responsible vendor or impacted organization. These flaws can also be discovered and exploited by criminals and foreign governments' intelligence services and militaries that will not responsibly disclose the flaws, but rather, will exploit them for their own gain.

AMERICAN CIVIL LIBERTIES UNION
WASHINGTON
LEGISLATIVE OFFICE
915 15th STREET, NW, 6TH FL
WASHINGTON, DC 20005
T/202.544.1681
F/202.546.0738
WWW.ACLU.ORG

MICHAEL W. MACLEOD-BALL
ACTING DIRECTOR

NATIONAL OFFICE
125 BROAD STREET, 18TH FL.
NEW YORK, NY 10004-2400
T/212.549.2500

[1] *Nat'l Telecomms. and Info. Admin*., 80 Fed. Reg. 53, 14360 (Mar. 19, 2015), http://www.ntia.doc.gov/files/ntia/publications/cybersecurity_rfc_03192015.pdf ("Vulnerability Disclosure. The security of the digital economy depends on a productive relationship between security vendors and researchers of all types who discover vulnerabilities in existing technology and systems, and the providers, owners, and operators of those systems. How can stakeholders build on existing work in this space to responsibly manage the vulnerability disclosure process without putting consumers at risk in the short run?").

[2] Gabe Rottman, Cybersecurity Doesn't Have to Mean Sacrificing Privacy, *Free Future*, January 13, 2015, https://www.aclu.org/blog/cybersecurity-doesnt-have-mean-sacrificing-privacy

There are many barriers that can prevent researchers from notifying the company or developers responsible for the flawed code. It can be difficult to discover the contact information for an organization's information security team; reports of security flaws can sometimes result in legal threats from companies that think that by threatening the researchers, they can suppress the eventual public disclosure of the vulnerability; and the financial rewards for selling a vulnerability to an exploit broker, defense contractor or a government can result in a researcher having to choose between significant financial gain and a more secure internet.

The technology community has recognized these issues, and increasingly, many technology companies have embraced policies intended to incentivize the disclosure of vulnerabilities by researchers. These companies have learned that it is better to work with the computer security research community than to work against it. By making it easier for researchers to report security vulnerabilities, assuring researchers that they will not face legal threats, and rewarding researchers with bounties, several of the biggest technology companies have created an environment that encourages and rewards researchers who are trying to do the right thing.

Unfortunately, while security researcher-friendly policies are increasingly becoming the norm among tech companies, the federal government has yet to catch up. It can be extremely difficult, if not impossible, to discover contact information for the information security teams within federal agencies; researchers face legal risks and the possibility of an investigation by law enforcement agencies when they do report flaws that impact government systems; and, even though the U.S. government is reported to be a significant player in the market for security vulnerabilities, it has yet to embrace "bug bounties" (i.e., financial rewards for the discovery and disclosure of vulnerabilities) for flaws in U.S. government websites and systems.

We urge the Task Force to recommend that companies and government agencies alike adopt these industry best practice policies to incentivize reports from security researchers.

I. Publish Contact Information for Agencies' Information Security Teams

Researchers who discover a serious security flaw in a piece of software or website should not have to spend hours or days searching for the contact information for the information security team at the company or organization responsible for the vulnerable code.

Many large technology companies publish easily accessible contact information for their information security teams. These include Google,[3] Twitter,[4] Facebook,[5] Microsoft,[6] and Apple.[7] In the past, most companies published an email address (and a corresponding email encryption key) through which researchers were encouraged to submit vulnerability reports. Many companies have transitioned to HTTPS based web submissions for vulnerability reports, thereby

[3] *Application Security*, Google, http://www.google.com/about/appsecurity/ (last visited May 12, 2015).
[4] *Twitter*, Hacker One, https://hackerone.com/twitter (last visited May 12, 2015).
[5] *Whitehat*, Facebook, *https*://www.facebook.com/whitehat (last visited May 12, 2015).
[6] *Security TechCenter*, Microsoft, https://technet.microsoft.com/en-us/security/ff852094.aspx (last visited May 12, 2015).
[7] *Apple Product Security*, Apple, https://www.apple.com/support/security/ (last visited May 12, 2015).

ensuring that all reports are transmitted securely, instead of only those submitted by researchers who take the time to use email encryption.[8]

Providing security researchers with an easy way to report vulnerabilities is not just an industry best practice,[9] it is now a key component of what the Federal Trade Commission considers "reasonable and appropriate security."[10]

Although some federal agencies, such as the National Aeronautics and Space Administration (NASA),[11] the Department of Health and Human Services (HHS),[12] the Department of Housing and Urban Development (HUD),[13] and the Federal Energy Regulatory Commission (FERC)[14] have published contact information for their information security teams or chief information security officer, these agencies are the exception rather than the norm. Most agencies do not have such information posted on their websites, and of those that do, few solicit reports of security vulnerabilities from the research community. For now, the only way for the researchers to report vulnerabilities in most federal agency websites is to go through the United States Computer Emergency Readiness Team US-CERT.[15]

II. Responsible Disclosure Policies

Computer security researchers often face the risk of legal threats from the companies and organizations when they discover flaws in their software. Rather than focusing energy on promptly fixing their vulnerable software, some companies use legal threats or litigation to prevent the researcher from going public with information about the vulnerability, or to punish the researcher and send a signal to others in the community.[16]

---

[8] This includes Google, Facebook and all of the companies that now use Hacker One.

[9] *See ISO/IEC 29147:2014,* Int'l Org. for Standardization (Feb. 15, 2014), http://www.iso.org/iso/catalogue_detail.htm?csnumber=45170.

[10] *See* Complaint at 2, *HTC America Inc.*, FTC No. 122 3049 (June 25, 2013), *available at* https://www.ftc.gov/sites/default/files/documents/cases/2013/07/130702htccmpt.pdf (HTC "engaged in a number of practices that, taken together, failed to employ reasonable and appropriate security in the design and customization of the software on its mobile devices. Among other things [HTC] . . . failed to implement a process for receiving and addressing security vulnerability reports from third-party researchers, academics or other members of the public, thereby delaying its opportunity to correct discovered vulnerabilities or respond to reported incidents.").

[11] *IT Security Division*, NASA, http://www.nasa.gov/offices/ocio/itsecurity (last visited May 12, 2015).

[12] *Information Security and Privacy Program*, U.S. Department of Health & Human Services, http://www.hhs.gov/ocio/securityprivacy/ (last visited May 12, 2015).

[13] *Chief Information Officer Functional Points of Contact*, U.S. Dep't of Housing and Urban Dev't, http://portal.hud.gov/hudportal/HUD?src=/program_offices/cio/dircio (last visited May 12, 2015).

[14] *Information Security and Systems Assurance Division*, Fed. Energy Regulatory Comm'n, http://www.ferc.gov/about/offices/oed/oed-io/oed-sys-security.asp (last visited May 12, 2015).

[15] *Report a Vulnerability,* Vulnerability Notes Database, http://www.kb.cert.org/vuls/html/report-a-vulnerability/ (last visited May 12, 2015).

[16] *See generally* Derek E. Bambauer and Oliver Day, *The Hacker's Aegis*, Emory L.J. 60, 1051 (Mar. 1, 2010), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1561845.

These legal risks can chill legitimate security research and force researchers to spend significant time and money seeking legal advice.[17]

In an effort to encourage and not discourage security research, several technology companies have in recent years established *responsible disclosure policies*, through which these firms promise that they will neither sue nor report the researchers to law enforcement authorities as long as the individuals who discovered the flaw provide the company time fix the flaw before they release information about it to the public. A number of major technology companies have adopted such policies, including Facebook, [18] GitHub,[19] DropBox,[20] NetFlix,[21] and Tesla Motors.[22]

We are not aware of any U.S. government agency that has published a responsible disclosure policy, and we urge you to issue a recommendation that they do so.

III. Bounty Programs

For far too long, researchers who discovered a security vulnerability have had to make a difficult choice: do the right thing—by telling the company responsible for the software or warning the general public—or sell the vulnerability, often to a government, which would then quietly exploit that flaw for its own gain.[23]

In an effort to disrupt this shadowy grey market and to provide some financial reward to researchers who notify the responsible vendor or developers, some leading technology companies have created "bug bounty" programs. These programs, which have been adopted by Google,[24] Microsoft,[25] Facebook,[26] Yahoo,[27] Twitter,[28] Snapchat,[29] and others offer researchers thousands (and, in some cases, tens of thousands) of dollars per vulnerability.

---

[17] *See Long-Form Comment: Proposed Class 25: Security Research*, Exemption to Prohibition on Circumvention of Copyright Protection Sys. for Access Control Technologies, U.S. Copyright Office, No. 2014-07 (Feb. 6, 2015), *available at* http://copyright.gov/1201/2015/comments-020615/InitialComments_LongForm_Green_Class25.pdf.
[18] *Whitehat*, Facebook, https://www.facebook.com/whitehat (last visited May 12, 2015).
[19] *Responsible Disclosure Policy*, GitHub, https://github.com/blog/1069-responsible-disclosure-policy (last visited May 12, 2015).
[20] *Security and Privacy*, Dropbox, https://www.dropbox.com/en/help/4399 (last visited May 12, 2015).
[21] *Responsible Vulnerability Disclosure*, Netflix, https://help.netflix.com/en/node/6657 (last visited May 12, 2015).
[22] *Customer Privacy Policy*, Tesla Motors, https://www.teslamotors.com/about/legal (last visited May 12, 2015).
[23] *See* Charlie Miller, *The Legitimate Vulnerability Market: Inside the Secretive World of 0-day Exploit Sales*, Independent Security Evaluators (May 6, 2007), http://weis2007.econinfosec.org/papers/29.pdf.
[24] *Google Vulnerability Reward Program (VRP) Rules*, Google http://www.google.com/about/appsecurity/reward-program/ (last visited May 12, 2015) and *Chrome Reward Program Rules*, Google, http://www.google.com/about/appsecurity/chrome-rewards/ (last visited May 12, 2015).
[25] *Microsoft Bounty Programs*, Microsoft, https://technet.microsoft.com/en-us/library/dn425036.aspx (last visited May 12, 2015).
[26] *Whitehat*, Facebook, https://www.facebook.com/whitehat (last visited May 12, 2015).
[27] *Yahoo!*, Hacker One, https://hackerone.com/yahoo (last visited May 12, 2015).
[28] *Twitter*, Hacker One, https://hackerone.com/twitter (last visited May 12, 2015).
[29] *SnapChat*, Hacker One, https://hackerone.com/snapchat (last visited May 12, 2015).

Although the U.S. government is no stranger to paying for security vulnerabilities and exploits—it is reportedly the largest player in the commercial market for vulnerabilities[30]—these vulnerabilities are purchased in order to allow law enforcement and intelligence agencies to exploit the flaws, not to reward researchers for notifying the developers responsible for the software.

In spite of the billions of dollars spent annually by the U.S. government on cybersecurity,[31] we are not aware of any U.S government agency that has established a bug bounty program intended to reward researchers who find flaws in U.S. government systems and websites. Again, we urge you to recommend "bug bounties" as a government-wide best practice.

IV. Conclusion

It is imperative that government agencies and companies take every possible measure to both protect the security of their systems and websites, and to improve the process of computer security vulnerability disclosure in order to encourage the reporting of exploitable programming flaws and design mistakes. We believe that companies and government agencies have much to gain by working with, rather than against, the computer security research community.

Please do not hesitate to contact Christopher Soghoian at the ACLU with any questions. He can be reached at csoghoian@aclu.org.

Thank you,

Michael W. Macleod Ball
Acting Director, Washington Legislative Office

Christopher Soghoian, Ph.D.
Principal Technologist
Speech, Privacy & Technology Project

[30] Nicole Perlroth and David E. Sanger, *Nations Buying as Hackers Sell Flaws in Computer Code*, N.Y. Times, July 13, 2013, http://www.nytimes.com/2013/07/14/world/europe/nations-buying-as-hackers-sell-computer-flaws.html?_r=0 and *The Digital Arms Trade*, The Economist, Mar. 30, 2013, http://www.economist.com/news/business/21574478-market-software-helps-hackers-penetrate-computer-systems-digital-arms-trade.

[31] Aliya Sternstein, *Federal Cybersecurity Spending is Big Bucks. Why Doesn't It Stop Hackers?*, Nextgov (Jan. 8, 2015), http://www.nextgov.com/cybersecurity/2015/01/has-spending-nearly-60-billion-federal-cybersecurity-stopped-hackers/102534/.