RAPID7

Statement of Harley Geiger
Director of Public Policy
Rapid7

Hearing on Strengthening the Cybersecurity of the Internet of Things

Before the Committee on Commerce, Science, and Transportation
Subcommittee on Security
US Senate

April 30th, 2019

Chairman Sullivan, Ranking Member Markey, and Members of the Subcommittee: Thank you for inviting me to provide testimony on this important issue on behalf of Rapid7. Rapid7 is a cybersecurity and data analytics firm headquartered in Boston, MA, with offices around the world. Rapid7's solutions manage cybersecurity risk and simplify the complex, allowing security teams to work more effectively with IT and development to reduce vulnerabilities, monitor for malicious behavior, investigate and shut down attacks, and automate routine tasks. Over 7,800 customers worldwide rely on Rapid7 technology, services, and research to improve cybersecurity outcomes, protect consumers, and securely advance their organizations.

Introduction

The Internet of Things (IoT) has great potential for technological innovation, economic growth, and enhanced quality of life. To reap these benefits while safeguarding consumers, businesses, and infrastructure, comprehensive cybersecurity protections will be needed. Many of the technical and policy issues related to IoT are not unique to this field. However, the diversity and quantity of IoT devices apply familiar cybersecurity problems to new business sectors at a larger scale.

Broad deployment of IoT will grow the risk of breach of personal information and create a much larger attack surface for malicious actors. Security vulnerabilities that once affected laptops and smartphones can now affect refrigerators, implantable medical devices, automobiles, and more. High-profile examples of this concern include IoT devices infected by malware and leveraged to launch powerful attacks that disrupted internet service in large swathes of the US.[1] Digital devices are coming online at an unprecedented rate, and a failure to

[1] Nicole Perlroth, Hackers Used New Weapons to Disrupt Major Websites Across U.S., New York Times, Oct. 21, 2016, https://www.nytimes.com/2016/10/22/business/internet-problems-attack.html.

integrate reasonable security standards now will create a wave of cybersecurity exposure that will linger in enterprises, households, and infrastructure for some time.[2]

There is growing recognition that purely voluntary risk management of IoT by the private sector is not adequately effective, and that government needs to facilitate or mandate adoption of basic security. An endless push for more voluntary guidance or frameworks delays meaningful security requirements and enforcement. Policymakers have recognized the issue and are starting to take action – at the federal and state level, in the Executive and Legislative Branches, as well as internationally. However, the drive for governments to take a more active role must also be balanced against the risk of a fragmented or overly prescriptive regulatory landscape. The sheer complexity of laws can itself be a barrier to security.

Nonetheless, the federal government need not — and should not — accept the premise that its only role in IoT security is that of a convener. Nor would innovation be irreparably stifled by advancing security or transparency baselines for devices that collect intimate details about consumers and whose collective computing power can form a weapon that threatens critical infrastructure.

Rapid7 has four recommendations for Congress:

1) **Require reasonable security of personal information.** Security of personal information is fundamental to privacy and should be included in any privacy legislation. Legislation that requires risk-based security requirements for personal information will apply to IoT devices collecting and processing that information. This will strengthen some aspects of IoT security in sectors that are otherwise not covered by the jurisdiction of federal agencies.

2) **Support coordinated but enforceable agency actions on IoT security based on industry standards.** Federal agencies should be empowered to require reasonable security for IoT, including security-by-design principles, within their areas of jurisdiction. To the extent possible, agency requirements should be harmonized by following a consistent baseline supported by industry standards. Voluntary guidance should not replace formal accountability and enforcement mechanisms when baseline security is not met. Congress should exercise its oversight role to ensure agency efforts are effective in strengthening IoT security.

3) **Facilitate voluntary transparency programs for consumer IoT security.** Congress should support voluntary consumer awareness programs to enhance the transparency of critical security features of consumer IoT devices, such as certifications, seals, or labels. Providing consumers with clear information about critical security features in IoT devices will foster market competition based on security, promote innovation in security, and build trust in the security of IoT products.

[2] Gartner estimates 25 billion connected devices will be in use by 2021. Gartner Identifies Top 10 Strategic IoT Technologies and Trends, Gartner, Nov. 7, 2018, https://www.gartner.com/en/newsroom/press-releases/2018-11-07-gartner-identifies-top-10-strategic-iot-technologies-and-trends.

4) **Avoid new regulations that chill beneficial security research.** Any new regulations related to IoT should not undermine cybersecurity by imposing blanket access and use restrictions that hinder independent research and repair. Independent security researchers, acting in good faith, that identify and disclose vulnerabilities in coordination with IoT manufacturers can advance security by boosting the likelihood of remediating otherwise unaddressed vulnerabilities.

I. IoT Security Challenges

1. "The Internet of Things" encompasses many technologies

The great variety of IoT devices is a key consideration for policymaking around security. IoT systems can vary considerably from one another, particularly consumer versus industrial applications, and so can their security needs. Because of this, there is no one-size-fits-all solution to IoT security, though some basic security features that are based on outcomes and existing standards can apply to many devices.

An "Internet of Things" device generally refers to a physical object that contains a CPU and memory, runs software, communicates with other devices electronically, and typically uses sensors to collect data about its status or environment. This concept encompasses a huge range of computers — large and expensive objects such as vehicles and industrial robots, as well as small and inexpensive objects such as light bulbs and baby monitors. The security risks, and the potential consequences of security failures, vary across so many different deployments.

It is also critical to recognize that IoT devices typically do not stand alone. Instead, IoT devices are often part of a broader ecosystem with several components: distributed sensors gathering data for the device, the network transmitting data, cloud storage of data gathered by the device, a mobile app for external management and control, companion devices, etc. These components can have their own security issues that implicate the rest of the ecosystem — for example, device security features will not necessarily prevent attacks on a weak mobile app or sensitive data from leaking from improperly configured cloud storage.[3] In isolation, security features on the device itself will have limited effectiveness.

2. Common vulnerabilities and exposures

Because IoT devices do not normally look or behave like traditional computers, they are often marketed and treated as if they are single-purpose devices, rather than the general-purpose computers they actually are. In addition, IoT brings connectivity to more business sectors that

[3] Tod Beardsley, R7-2018-52: Guardzilla IoT Video Camera Hard-Coded Credential (CVE-2018-5560), Rapid7, Dec. 27, 2018, https://blog.rapid7.com/2018/12/27/r7-2018-52-guardzilla-iot-video-camera-hard-coded-credential-cve-2018-5560.

previously did not provide networked products and have less experience with managing cybersecurity risks. As a result, basic precautions to thwart casual attackers that manufacturers might take with traditional computers can fail to make it into production of IoT devices.

The items below describe some common vulnerabilities and exposures for IoT devices we have encountered. Not all IoT devices suffer from all of these issues, but in our experience, it is common to find consumer-grade IoT devices that exhibit at least one serious failing.

a) **Lack of security for stored data:** IoT devices and related services often fail to store data in industry-standard, encrypted formats — both if data is captured on the device or held in the cloud.[4] Failure to protect stored data with cryptography risks breach of the data. This feature is particularly important if the stored data is sensitive or personal to the user.

b) **Lack of security for data in transit:** IoT devices often fail to use modern cryptographic standards or fail to authenticate properly, risking exposure of user data in transport over both the public internet and local area networks.[5] This puts the device at greater risk of many active and passive network attacks, which could otherwise be defeated with widely used communication encryption protocols like Transport Layer Security (which, among other things, underpins HTTPS).

c) **Weak credentials:** IoT manufacturers occasionally include default or service accounts, which are either difficult or impossible to disable under normal usage. These accounts often use default or easily guessable passwords, and tend to share the same password, key, or token across many devices.[6] Weak credentials raise the risk that the device can be accessed and controlled by unauthorized users.[7]

d) **Mobile application access:** Many IoT devices include a mobile app for external management and control. Improperly secured mobile applications can be exploited to provide unauthorized users with control of the device.[8] Some mobile applications are also granted more access rights to a device than what is needed for the

[4] Daniel Oberhaus, This Hacker Showed How a Smart Lightbulb Could Leak Your Wi-Fi Password, Jan. 31, 2019, https://motherboard.vice.com/en_us/article/kzdwp9/this-hacker-showed-how-a-smart-lightbulb-could-leak-your-wi-fi-password.
[5] Iain Thomson, Wi-Fi baby heart monitor may have the worst IoT security of 2016, The Register, Oct. 13, 2016, https://www.theregister.co.uk/2016/10/13/possibly_worst_iot_security_failure_yet.
[6] "Based on field experience, passwords for approximately 15 out of 100 devices have never been changed from their default values. And just the five most popular user name/password pairs are enough to get admin access to 1 out of every 10 devices." Positive Technologies, Practical ways to misuse a router, Jun. 16, 2017, http://blog.ptsecurity.com/2017/06/practical-ways-to-misuse-router.html.
[7] Dan Goodin, Leak of >1,700 valid passwords could make the IoT mess much worse, Ars Technica, Aug. 25, 2017, https://arstechnica.com/information-technology/2017/08/leak-of-1700-valid-passwords-could-make-the-iot-mess-much-worse.
[8] Andy Greenberg, This Gadget Hacks GM Cars To Locate, Unlock, And Start Them, Jul. 30, 2015, https://www.wired.com/2015/07/gadget-hacks-gm-cars-locate-unlock-start.

application to function properly.[9]

e) **Lack of segmentation:** When different components of a device share the same memory or circuitry, a flaw in one component can lead to exploitation of another component. For example, an attack on the infotainment system of a vehicle can lead to access of the critical driving functions, such as acceleration or braking.[10] Non-critical controls should be physically and logically separated from systems implicating safety.

f) **UART access:** Universal Asynchronous Receiver/Transmitter (UART) interfaces often enable a physically close attacker to access and alter IoT devices in ways that bypass the normal authentication mechanisms via a serial cable connection.[11] In addition, UART interfaces tend to grant root access, far exceeding the permissions of regular users, which can enable persistent attacks on devices.

g) **Insufficient update practices:** IoT devices, unlike most traditional computers, can lack an effective update and upgrade path once the devices leave the manufacturer's warehouse. In some cases, the manufacturer may no longer provide security support (such as patches) after a device outlives its designated shelf life.[12] Without a patching capability, it is difficult to correct devices' known security flaws at a large scale, leaving the devices vulnerable to repeated attacks even when a fix is available.[13] This issue is more prevalent in inexpensive consumer devices that use commodity components, rather than more sophisticated systems.

We do not believe the technical challenges to providing basic security for the majority of IoT devices and associated technologies are insurmountable at present. We are optimistic that reasonably secure IoT deployments will become more common in the future, but we believe it is essential that IoT manufacturers be incentivized to incorporate widely acknowledged security protections from the design phase forward.

---

[9] Dan Goodin, Samsung Smart Home flaws let hackers make keys to front door, Ars Technica, May 2, 2016, https://arstechnica.com/information-technology/2016/05/samsung-smart-home-flaws-lets-hackers-make-keys-to-front-door.

[10] Andy Greenberg, Hackers Remotely Kill A Jeep On The Highway - With Me In It, Wired, Jul. 21, 2015, https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway.

[11] Mark Stanislav and Tod Beardsley, Hacking IoT: A Case Study on Baby Monitor Exposures and Vulnerabilities, Rapid7, Sep. 2015, https://www.rapid7.com/docs/Hacking-IoT-A-Case-Study-on-Baby-Monitor-Exposures-and-Vulnerabilities.pdf.

[12] See, e.g., Letter from Mary Engle to Richard J. Lutton, Jr. re: Nest Labs, Inc., FTC File No. 162-3119, Jul. 7, 2016, https://www.ftc.gov/system/files/documents/closing_letters/nid/160707nestrevolvletter.pdf. See also Jessica Rich, What happens when the sun sets on a smart product?, Fed. Trade Commission, Jul. 13, 2016, https://www.ftc.gov/news-events/blogs/business-blog/2016/07/what-happens-when-sun-sets-smart-product.

[13] Troy Hunt, Data from connected CloudPets teddy bears leaked and ransomed, exposing kids' voice messages, Feb. 28, 2017, https://www.troyhunt.com/data-from-connected-cloudpets-teddy-bears-leaked-and-ransomed-exposing-kids-voice-messages.

II. Recommendations for Congress

1. Legislation to require reasonable security for personal information

Rapid7 strongly supports a national framework requiring reasonable security for consumers' personal information.[14] As Congress considers privacy legislation, it is critical that security of personal information be included, as security is fundamental to privacy.[15] Many of the concerns and events driving the privacy debate, such as accidental data breach or malicious hacking, are a result of security failures, not failures of notice, choice, transparency, or discriminatory use of data.[16] However, if federal privacy legislation once again fails to move forward, we would urge a standalone legislative effort to advance risk-based security for personal information.

Legislation establishing an affirmative security obligation for entities collecting and processing personal information would prompt some basic security improvements to IoT devices that collect and process such information. Numerous, though not all, IoT security vulnerabilities involve unauthorized exposure of data that is typically categorized as "personal information" in data security laws, such as audio and visual recordings, credentials (username and password providing access to an online account), and geolocation data. Because the requirement of reasonable security would be tied to personal information, rather than a definition of IoT, it would cut across IoT deployments in disparate sectors and encompass the other technologies (such as cloud storage) that integrate with the IoT device.[17]

There is a great deal of precedent available for reasonable security requirements. Half of US states have a data security requirement for personal information held by the private sector,[18] as does the European Union's (EU) General Data Protection Regulation.[19] Similar requirements are well-established in sectoral privacy regulation, such as under COPPA,[20] GLBA,[21] and HIPAA.[22] What is missing outside of those sectors is a nationwide affirmative obligation for reasonable security of personal information in the US. This would provide more consistent

---

[14] Harley Geiger, Updating Data Security Laws - A Starting Point, Rapid7, May 4, 2018, https://blog.rapid7.com/2018/05/04/updating-data-security-laws-a-starting-point.
[15] See e.g., background of Fair Information Practice Principles: Department of Homeland Security, Privacy Policy Guidance Memorandum, Dec. 29, 2008, https://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf.
[16] See, e.g., The Equifax Data Breach, U.S. House of Representatives, Committee on Oversight and Government Reform, Majority Staff Report, Dec. 2018, pg. 4, https://republicans-oversight.house.gov/wp-content/uploads/2018/12/Equifax-Report.pdf.
[17] Federal Trade Commission Staff Report, Internet of Things – Privacy & Security in a Connected World, pg. 49, https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.
[18] http://www.ncsl.org/research/telecommunications-and-information-technology/data-security-laws.aspx
[19] Article 32. https://gdpr-info.eu/art-32-gdpr/
[20] Children's Online Privacy Protection Act, 16 CFR 312.8.
[21] Gramm-Leach-Bliley Act, 16 CFR 314.
[22] Health Insurance Portability and Accountability Act, 45 CFR 164.306.

expectations for businesses and more consistent protection for consumers. However, if the patchwork of current data security laws is preempted, a federal replacement should not establish substantially weaker protections than the status quo.[23]

Breach notification requirements only apply *after* a breach has occurred. Data security safeguards are critical to preventing breaches *before* they occur by addressing the root cause of many breaches: inadequate security. Too often, breach notification requirements are relied on as a substitute for data security — since complying with breach notification requirements is expensive and difficult, organizations will be inspired to implement strong security safeguards to prevent breaches. Yet this approach is not adequate – as demonstrated by the continued march of severe data breaches caused by poor security, in spite of all enactment of breach notification laws in all 50 states. A requirement of reasonable security for personal information is distinct from breach notification, and should be considered separately.

Privacy legislation that fails to integrate security will have negative consequences for consumers. Unfortunately, this is occurring in several states that are among the half without data security laws – most notably the Washington Privacy Act,[24] but also legislation in Illinois, Montana, New Jersey, North Dakota, and others.[25] Some of these efforts copycat the California Consumer Privacy Protection Act, which did not include data security provisions – but California already has a data security law.[26] This problem will be especially serious if a federal privacy bill excludes security provisions but preempts state security laws.

2. Support coordinated but enforceable agency actions on IoT security based on industry standards

Recognizing the differences in IoT systems, we do not recommend Congress attempt prescriptive IoT-specific legislation at this time. Instead, regulatory efforts should be undertaken by agencies that already oversee those sectors and have deep knowledge of their practices. Ideally, regulatory bodies would work in a coordinated fashion to achieve consistency where possible. Congress should support agencies' efforts and exercise its oversight role to ensure their activities are effective in appropriately advancing reasonable IoT security.

Several agencies have started the work of articulating how IoT security fits within their authorities. Examples include the Food and Drug Administration,[27] the National Highway

---

[23] In particular, we urge that a federal baseline be risk-based, not be limited to protecting against economic or physical harm, avoid requiring real names to qualify as "personal information," and incentivize use of encryption. Harley Geiger, Updating Data Security Laws – A Starting Point, Rapid7, May 4, 2018, https://blog.rapid7.com/2018/05/04/updating-data-security-laws-a-starting-point.

[24] Washington Privacy Act, SB.5376, Feb. 18, 2019, http://lawfilesext.leg.wa.gov/biennium/2019-20/Pdf/Bills/Senate%20Bills/5376-S.pdf.

[25] Respectively: SB.1502 (IL), HB.457 (MT), S.2834 (NJ), HB.1485 (ND).

[26] CA Civ. Code 1798.81.5(b)

[27] FDA, Content of Premarket Submissions for Management of Cybersecurity of Medical Devices, Draft Guidance, Oct. 18, 2018, https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM623529.pdf. See also, Food and Drug Administration, Postmarket Management for Cybersecurity in Medical Devices,

Transportation Administration,[28] the Consumer Product Safety Commission,[29] the Federal Energy Regulatory Commission,[30] the Federal Trade Commission,[31] and the Department of Defense.[32] Many of these efforts are voluntary but provide insight into how agencies expect IoT manufacturers and operators to mitigate basic security risks.

Congress should encourage other agencies to provide explicit guidance and, where appropriate, enforceable rules regarding the security of internet-connected devices under their jurisdiction. For example, the Federal Aviation Administration's cybersecurity expectations for unmanned aircraft should be clear, as should the Office of Management and Budget's security standards for IoT devices procured by the federal government. If there is a gap in authority, or if existing standards are unacceptably weak, Congress should consider legislation to prompt agency action without being overly prescriptive.[33]

NIST's work on authoritative, voluntary standards is extremely useful. NIST has dozens of initiatives related to IoT security, with about a dozen more planned.[34] NIST's ongoing work to define a "Core Security Capability Baseline" will help establish minimum security-by-design practices that should apply to the vast majority of IoT devices.[35] This can further inform expectations in consumer, federal, and industrial contexts. Rapid7's suggestions for these baseline capabilities have been the following:

1. **Asset identification:** The IoT device can be identified on a network.
2. **Update capability:** The IoT device's software and firmware can be updated post-market via a secure process.

Dec. 28, 2016, https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm482022.pdf.

[28] NHTSA, Cybersecurity Best Practices for Modern Vehicles, Oct. 15, 2016, https://www.nhtsa.gov/staticfiles/nvs/pdf/812333_CybersecurityForModernVehicles.pdf.

[29] CPSC, Statement of Commissioner Kaye, Regarding A Framework Of Safety For The Internet Of Things, Jan. 31, 2019, https://www.cpsc.gov/s3fs-public/A_Framework_for_Safety_Across_the_Internet_of_Things_1-31-2019_0.pdf.

[30] 18 CFR 40.

[31] Kristin Cohen and Peder Magee, FTC updates COPPA compliance plan for business, Federal Trade Commission, Jun. 21, 2017, https://www.ftc.gov/news-events/blogs/business-blog/2017/06/ftc-updates-coppa-compliance-plan-business. Federal Trade Commission, *Careful Connections, Building Security in the Internet of Things*, Jan. 2015, https://www.ftc.gov/system/files/documents/plain-language/pdf0199-carefulconnections-buildingsecurityinternetofthings.pdf.

[32] DoD CIO, Policy Recommendations for the Internet of Things, U.S. Department of Defense, December 2016, pg. 6, https://www.hsdl.org/?view&did=799676.

[33] For example, Rapid7 supports initiating clear standards for federal government procurement of IoT, which is the aim of S.734, the IoT Cybersecurity Improvement Act of 2019. Jen Ellis, The IoT Cybersecurity Improvement Act of 2019, Rapid7, Mar. 27, 2019, https://blog.rapid7.com/2019/03/27/the-iot-cybersecurity-improvement-act-of-2019.

[34] NIST, IoT Cybersecurity-Related Initiatives at NIST, Apr. 11, 2018, https://www.nist.gov/itl/applied-cybersecurity/nist-initiatives-iot.

[35] Dept. of Commerce, A Road Map Toward Resilience Against Botnets, Nov. 29, 2018, https://www.commerce.gov/sites/default/files/2018-11/Botnet%20Road%20Map%20112918%20for%20posting_0.pdf.

3. **Secure sensitive information:** The IoT device can use cryptography to secure stored and transmitted personally identifiable information, safety-critical information, credentials, or otherwise sensitive data.
4. **No shared credentials:** The IoT device does not use a default credential that is shared by many other IoT devices or is widely known.[36]
5. **Vulnerability handling:** The manufacturer should have an administrative process for accepting unsolicited vulnerability reports and acting on them.

However, it is important to point out that the above baseline features are already incorporated into many IoT standards and best practices documents. Government agencies, trade groups, and standards bodies have released a host of guidance and best practices for mitigating IoT security risks.[37] In fact, these are established best practices for traditional technologies, not just IoT.[38] As a result, Congress should be skeptical of claims that it is necessary to wait for the development of additional standards or best practices in order to have an expectation that the vast majority of IoT devices meet these basic features.

3. Facilitate voluntary transparency programs for security of consumer IoT

Rapid7 recommends Congress support voluntary processes that enhance the transparency of critical security features of consumer IoT devices. Consumer awareness plays an important role in IoT security, and end users would ideally evaluate device security as a routine part of purchasing. Yet consumers often have little insight into the presence of security features in an IoT device prior to purchase, which hinders informed buying decisions. Providing consumers with clear information about critical security features in IoT devices will foster market competition based on security, promote innovation in security, and build trust in the security of IoT products.

To help address this lack of transparency, numerous government and private-sector efforts aim to provide an IoT security certification or seal – similar to Energy Star, the recycling symbol, or nutrition labels. The National Telecommunications and Information Administration facilitated the successful completion of a transparency proposal focused on IoT security update capability and end-of-life.[39] Recently, the Departments of Commerce and Homeland

---

[36] California passed this requirement into law Sep. 28, 2018. It goes into effect in 2020. California SB 327, Sec. 1, https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB327.

[37] In addition to the guidance cited elsewhere in the testimony, see also: US Department of Homeland Security, Strategic Principles for Securing the Internet of Things (IoT), Nov. 15, 2016, https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL....pdf. United Kingdom Department for Digital, Culture Media, & Sport, Code of Practice for Consumer IoT Security, Oct. 14, 2018, https://www.gov.uk/government/publications/code-of-practice-for-consumer-iot-security. Microsoft, Security best practices for Internet of Things (IoT), Oct. 8, 2018, https://docs.microsoft.com/en-us/azure/iot-fundamentals/iot-security-best-practices. Online Trust Alliance, OTA IoT Trust Framework v2.5, May 22, 2018, https://www.internetsociety.org/iot/trust-framework.

[38] See, e.g., Council to Secure the Digital Economy, International Anti-botnet guide, 2018, https://securingdigitaleconomy.org/wp-content/uploads/2018/11/CSDE-Anti-Botnet-Report-final.pdf.

[39] The document was produced as part of a consensus-based multistakeholder process. National Telecommunications and Information Administration, Communicating IoT Device Security Update Capability to Improve Transparency for Consumers, Jul. 18, 2017,

Security released their "Botnet Roadmap," which includes planned projects related to labeling and assessment programs for both consumer and industrial IoT.[40] The EU Cybersecurity Act will also establish voluntary certification schemes for IoT, as well as other ICT products and services. Per the EU Cybersecurity Act, the certification schemes must designate basic, substantial, or high levels of security, with reference to available standards.[41] These schemes aim to strengthen the overall level of security in the EU and enable consumers to accurately gauge the relative security of certified products.[42]

In addition to these important efforts, we are encouraged that Congress is also exploring market-based means to bring information about the security of IoT products to the attention of consumers.[43] Senator Markey's Cyber Shield Act would require the Department of Commerce to convene public- and private-sector experts to establish security benchmarks for select connected products. The working group would be encouraged to incorporate existing standards rather than create new ones, and the benchmark would change over time to keep pace with evolving threats and expectations. The process, like that which produced the NIST Cybersecurity Framework, would be open for public review and comment. Manufacturers may voluntarily display "Cyber Shield" labels on IoT products that meet the security benchmarks (as certified by an accredited testing entity).[44]

The approach is not without its challenges. To be effective, the security benchmarks must be clear and focused, and consumers should recognize the certification or seal does not promise complete security. The program would need buy-in from security experts and responsible manufacturers. Nonetheless, strengthening the IoT ecosystem will require a multi-pronged approach from policymakers, and Rapid7 believes initiatives like these can be very useful tools for empowering consumers.

4. Avoid chilling independent security research

IoT security risks can prompt regulatory proposals to block access to device software unless authorized by the manufacturer or operator. Rapid7 believes this approach would be misguided. While safety and crime deterrence is certainly an important consideration for IoT, any new regulations related to IoT should not undermine cybersecurity by imposing blanket access and use restrictions that chill independent research and repair. Independent security researchers will be critical to match the greater need for security as IoT devices are more

---

https://www.ntia.doc.gov/files/ntia/publications/communicating_iot_security_update_capability_for_consumers_-_jul_2017.pdf.

[40] Completion of this work is not expected until mid-2021. Dept. of Commerce, A Road Map Toward Resilience Against Botnets, Nov. 29, 2018, pgs. 5-8, https://www.commerce.gov/sites/default/files/2018-11/Botnet%20Road%20Map%20112918%20for%20posting_0.pdf.

[41] See Articles 46, 51-54. European Parliament, Cybersecurity Act, Adopted Text, Mar. 12, 2019, http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P8-TA-2019-0151+0+DOC+PDF+V0//EN.

[42] *Id.*, Recitals 6-10.

[43] Harley Geiger, Legislation to Strengthen IoT Marketplace Transparency, Jun. 26, 2017, https://blog.rapid7.com/2017/06/26/legislation-to-strengthen-iot-marketplace-transparency.

[44] Cyber Shield Act of 2017, S.2020, 115th Cong., Oct. 26, 2017.

widely deployed. Time and again, good-faith researchers or “white hat hackers” have discovered and reported IoT security vulnerabilities, prompting patches and other mitigations that ultimately protect consumers.

Several existing laws chill security research, which can hinder independent efforts to assess the security of IoT devices. The Computer Fraud and Abuse Act (CFAA), Section 1201 of the Digital Millennium Copyright Act (DMCA), and other laws contain broad prohibitions on access to computers and software.[45] Although we recognize the beneficial role of these laws in deterring cybercrime, balancing greater flexibility for independent research and repair with law enforcement needs is increasingly important as IoT proliferates faster than the cybersecurity workforce.

As compared to several years ago, policymakers more frequently recognize the value of independent security research. For example, in 2018, the U.S. Copyright Office renewed a temporary exemption to Sec. 1201 of the DMCA for security research,[46] and expressed support for making the security research protections permanent.[47] The Department of Justice strongly urged renewal and expansion of the DMCA protections for researchers.[48] Another example: In 2016, the state of Washington included helpful protections for white hat security researchers in the state's cybercrime laws.[49]

Other federal and state legislative proposals related to IoT would have imposed broad and redundant restrictions on access to connected devices. For example, in 2015, a House Energy and Commerce Subcommittee released draft legislation that would have levied heavy fines on anyone accessing car software without manufacturer authorization for any reason — regardless of whether the accessor had purchased the car, or if the car was accessed for cybersecurity research purposes.[50] The following year, a similar bill restricting access to vehicle software was introduced in the Michigan Senate.[51] Proposals such as these are not just overbroad, but also largely redundant of existing laws prohibiting unauthorized access and use of computers.[52]

Such restrictive proposals would hinder legitimate security researchers and repair services that can assess and fix the devices’ cybersecurity vulnerabilities. Security researchers identify errors and vulnerabilities in software, digital devices, and networks, and disclose them to

---

[45] Deirdre Mulligan, Nick Doty, and Jim Dempsey, Cybersecurity Research: Addressing the Legal Barriers and Disincentives, Berkeley Center for Law and Technology, Sep. 28, 2015, http://ondoc.logand.com/d/5689/pdf.
[46] Harley Geiger, Expanded Protections for Security Researchers Under DMCA Sec. 1201, Rapid7, Nov. 1, 2018, https://blog.rapid7.com/2018/11/01/expanded-protections-for-security-researchers-under-dmca-sec-1201.
[47] US Copyright Office, Section 1201 of Title 17, Report of the Register of Copyrights, Jun. 2017, pgs. 74-76, https://www.copyright.gov/policy/1201/section-1201-full-report.pdf.
[48] US Dept. of Justice, Letter from John Lynch (CCIPS) to Regan Smith (USCO), Jun. 28, 2018, https://www.copyright.gov/1201/2018/USCO-letters/USDOJ_Letter_to_USCO.pdf.
[49] Revised Code of Washington 9A.90.030(10)-(11).
[50] Harley Geiger, Draft Car Safety Bill Goes In The Wrong Direction, Center for Democracy & Technology, Oct. 20, 2015, https://cdt.org/blog/draft-car-safety-bill-goes-in-the-wrong-direction.
[51] Joint letter to Michigan Senator Mike Kowall "Re: Car Hacking Legislation – S.B. 0927 (2016)," May 16, 2016, https://www.rapid7.com/globalassets/_pdfs/policy/letter-re-sb-0927-from-cybersecurity-researchers-051616.pdf.
[52] *Id.*

prevent their exploitation by criminals. This research strengthens cybersecurity because the researchers call attention to vulnerabilities that manufacturers may have missed or ignored, which encourages manufacturers or other parties to make the appropriate fixes or mitigations to keep people safe. As the growth of IoT devices creates a larger attack surface for malicious actors, it will be crucial to foster an environment where good-faith disclosure of security issues in devices or systems is taken seriously and openly, rather than with threats or avoidance.[53]

* * *

We thank the Committee for holding this hearing and for providing us the opportunity to share our views.

[53] Cybersecurity Coalition, Policy Priorities for Coordinated Vulnerability Disclosure and Handling, Feb. 25, 2019, https://www.cybersecuritycoalition.org/policy-priorities.