CYBER STATECRAFT INITIATIVE

DFRLab

SECURITY IN THE BILLIONS:

Toward a Multinational Strategy to Better Secure the IoT Ecosystem

Patrick Mitchell, Liv Rowley, and Justin Sherman
with Nima Agah, Gabrielle Young, and Tianjiu Zuo

CYBER STATECRAFT
INITIATIVE

DFRLab

The Cyber Statecraft Initiative works at the nexus of geopolitics and cybersecurity to craft strategies to help shape the conduct of statecraft and to better inform and secure users of technology. This work extends through the competition of state and non-state actors, the security of the internet and computing systems, the safety of operational technology and physical systems, and the communities of cyberspace. The Initiative convenes a diverse network of passionate and knowledgeable contributors, bridging the gap among technical, policy, and user communities.

The mission of the **Digital Forensic Research Lab (DFRLab)** is to identify, expose, and explain disinformation where and when it occurs using open-source research; to promote objective truth as a foundation of government for and by people; to protect democratic institutions and norms from those who would seek to undermine them in the digital engagement space; to create a new model of expertise adapted for impact and real-world results; and to forge digital resilience at a time when humans are more interconnected than at any point in history, by building the world's leading hub of digital forensic analysts tracking events in governance, technology, and security.

This report is written and published in accordance with the Atlantic Council Policy on Intellectual Independence. The author is solely responsible for its analysis and recommendations. The Atlantic Council and its donors do not determine, nor do they necessarily endorse or advocate for, any of this report's conclusions.

ISBN-13: 978-1-61977-249-6

Atlantic Council
1030 15th Street NW, 12th Floor
Washington, DC 20005

For more information, please visit
www.AtlanticCouncil.org.

Cover image licensing language: CSI produced this report's cover image using in part OpenAI's DALL-E program, an AI image-generating application. Upon generating the draft image-prompt language, the authors reviewed, edited, and revised the language to their own liking and take ultimate responsibility for the content of this publication.

CYBER STATECRAFT INITIATIVE

DFRLab

SECURITY IN THE BILLIONS: Toward a Multinational Strategy to Better Secure the IoT Ecosystem

Patrick Mitchell, Liv Rowley, and Justin Sherman
with Nima Agah, Gabrielle Young, and Tianjiu Zuo

EXECUTIVE SUMMARY

The explosion of Internet of Things (IoT) devices and services worldwide has contributed to an explosion in data processing and interconnectivity. Simultaneously, this interconnection and resulting interdependence have amplified a range of cybersecurity risks to individuals' data, company networks, critical infrastructure, and the internet ecosystem writ large. Governments, companies, and civil society have proposed and implemented a range of IoT cybersecurity initiatives to meet this challenge, ranging from introducing voluntary standards and best practices to mandating the use of cybersecurity certifications and labels. However, issues like fragmentation among and between approaches, complex certification schemes, and placing the burden on buyers have left much to be desired in bolstering IoT cybersecurity. Ugly knock-on effects to states, the private sector, and users bring risks to individual privacy, physical safety, other parts of the internet ecosystem, and broader economic and national security.

In light of this systemic risk, this report offers a multinational strategy to enhance the security of the IoT ecosystem. It provides a framework for a clearer understanding of the IoT security landscape and its needs—one that focuses on the entire IoT product lifecycle, looks to reduce fragmentation between policy approaches, and seeks to better situate technical and process guidance into cybersecurity policy. Principally, it analyzes and uses as case studies the United States, United Kingdom (UK), Australia, and Singapore, due to combinations of their IoT security maturity, overall cybersecurity capacity, and general influence on the global IoT and internet security conversation. It additionally examines three industry verticals, smart homes, networking and telecommunications, and consumer healthcare, which cover different products and serve as a useful proxy for understanding the broader IoT market because of their market size, their consumer reach, and their varying levels of security maturity.

This report looks to existing security initiatives as much as possible—both to leverage existing work and to avoid counterproductively suggesting an entirely new approach to IoT security—while recommending changes and introducing more cohesion and coordination to regulatory approaches to IoT cybersecurity. It walks through the current state of risk in the ecosystem, analyzes challenges with the current policy model, and describes a synthesized IoT security framework. The report then lays out nine recommendations for government and industry actors to enhance IoT security, broken into three recommendation sets: setting a baseline of minimally acceptable security (or "Tier 1"), incentivizing above the baseline (or "Tier 2" and above), and pursuing international alignment on standards and implementation across the entire IoT product lifecycle (from design to sunsetting). It also includes implementation guidance for the United States, Australia, UK, and Singapore, providing a clearer roadmap for countries to operationalize the recommendations in their specific jurisdictions—and push towards a stronger, more cohesive multinational approach to securing the IoT worldwide.

ACKNOWLEDGMENTS

The authors thank Kat Megas, James Deacon, David Kleidermacher, and Rob Spiger for their comments on earlier drafts of this document and Trey Herr and Bruce Schneier for support. Thanks to Nancy Messieh for her support with data visualization. The authors also thank all the participants, who shall remain anonymous, in multiple Chatham House Rule discussions about the issues. Thank you to Nancy Messiah and Andrea Raitu for data visualization and web design and to Donald Partyka and Anais Gonzalez for graphic and document design.

TABLE OF CONTENTS

1. INTRODUCTION

The billions of Internet of Things (IoT) products used worldwide have contributed to an explosion in data processing and the connection of individuals, buildings, vehicles, and physical machines to the global internet. Work-from-home policies and the need for contact tracing during the COVID-19 pandemic have furthered societal dependence on IoT products. All this interconnection and interdependence have amplified a range of cybersecurity risks to individuals' data, company networks, critical infrastructure, and the internet ecosystem writ large.

Securing IoT products is inherently critical because IoT products increasingly touch all facets of modern life. Citizens have IoT wearables on their bodies and IoT products in their cars, gathering data on their heartbeats, footsteps, and Global Positioning System (GPS) locations. People also have IoT smart products in their homes—speakers awake to every private conversation, internet-connected door locks, devices that control atmospheric systems, and cameras to monitor young children and pets. Hospitals even use IoT products to control medicine dosages to patients. The ever-growing reliance on IoT products increasingly and inescapably ties users to network and telecommunications systems, including the cloud. IoT insecurity, given this degree of interconnection, poses risks to individual privacy, individual safety, and national security.

The IoT explosion is also poised to impact the security of the internet ecosystem writ large. More IoT products deploy each year, meaning IoT products constitute a significant percentage of devices linked to the global internet. For example, IoT Analytics, a market research firm, estimates that IoT products surpassed traditional internet-connected devices in 2019 and projects that the ratio will be around three to one by 2025.[1] At that scale, poorly secured products (for instance, those with easy-to-guess passwords or with known and unfixed security flaws) can enable attackers to gain footholds in corporate or otherwise sensitive environments and steal data or cause disruption. For instance, hackers could exploit security problems in IoT cameras to break into a building—digitally or physically.[2] Hackers can break into IoT devices at scale to launch distributed denial of service (DDoS) attacks that bring down internet services for hundreds of thousands or even millions of consumers.

In response to these cybersecurity risks, governments, private companies, industry organizations, and civil society groups have developed a myriad of national and industry frameworks to improve IoT security, each addressing considerations in the product design, development, sale and setup, maintenance, and sunsetting phases. These numerous controls sets and frameworks, however, are a hodgepodge across and within jurisdictions. Within jurisdictions, some governments are charging ahead with detailed IoT security guidance while others have made little substantive headway or have ambiguous policy goals that confuse and impede industry progress. Between jurisdictions, fragmented requirements have chilled efforts by even some of the most security-concerned vendors to act. Consumers, meanwhile, must grapple with IoT product insecurity, bad security outcomes, and ugly knock-on effects to others in their communities and networks—exacerbated by a lack of security information from vendors. Poor outcomes for users, a lack of cross-national harmonization, and gaps between government and industry efforts impede better security in the IoT ecosystem.

Yet, progress is possible. The number of countries and industry actors who have acknowledged one standard alone—European Norm (EN) 303 645, from the European Telecommunication Standards Institute (ETSI)—as a consensus approach alone demonstrates how some baseline security guidance can help drive real, coordinated change.

This report presents a consolidated approach to IoT cybersecurity to reconcile existing national approaches, balance the interest of public and private sectors, and ensure that a product recognized as secure in one jurisdiction will be recognized as secure in others. The framework is not prescriptive to the level of individual controls;

[1] Knud Lasse Lueth, "State of the IoT 2020: 12 Billion IoT Connections, Surpassing Non-IoT for the First Time," IoT-Analytics.com, November 19, 2020, https://iot-analytics.com/state-of-the-iot-2020-12-billion-iot-connections-surpassing-non-iot-for-the-first-time/.

[2] Keumars Afifi-Sabet, "Critical Supply Chain Flaw Exposes IoT Cameras to Cyber Attack," IT Pro, June 16, 2021, https://www.itpro.com/security/vulnerability/359899/critical-supply-chain-flaw-exposes-iot-cameras-to-cyber-attack.

rather, it seeks to address the structural priorities of approaches taken by industry coalitions and governments in the United States, United Kingdom (UK), Singapore, and Australia. We focus on these countries because of the maturity of their IoT cybersecurity approaches, their mature cyber policy processes, their historical influence on cybersecurity policy in other countries, and the strong precedent for cooperation across all four.

In considering the effects of this consolidated approach, the report also focuses on three verticals: smart homes, networking and telecommunications, and consumer healthcare. These three provide ready critical IoT product use cases, differentiate in the kinds of technology and products available, and serve as useful proxies for understanding the broader IoT market because of their market size, consumer reach, and varying levels of security maturity.

This report draws on research of IoT security best practices, standards, laws, and regulations; conversations with industry stakeholders and policymakers; and convenings with members of the IoT security community. In principle and wherever possible in practice, the report relies on existing approaches, seeking to create as little new information or guidance as practicable to ease implementation. The first section below describes the state of risk in the IoT ecosystem, including challenges with the current model, insecurity across three IoT industry segments, and a brief history of IoT security efforts and control sets across the United States, UK, Australia, and Singapore as well as industry-led efforts. The second section synthesizes these disparate control sets, mapped against every phase of the IoT product lifecycle. The third (and final section) presents a consolidated approach to IoT security across these four countries and the relevant industry partners—with nine recommendations to address gaps in existing IoT security approaches, disincentivize further fragmentation in standard setting or enforcement, and rationalize the balance between public and private sector security interests. These recommendations come with implementation guidance specific to each of the four countries.

While this report describes some key components of an IoT labeling approach, it deliberately does not prescribe a particular label design. The report leaves open many questions that require more work, including "who" sets label design, "how" companies should pair physical and digital labels, and to "what" extent companies and/or governments should harmonize labels across jurisdictions.

There is an overriding public interest in secure IoT products, and industry players—including source manufacturers, integrators/vendors, and retailers—must be responsive to this interest. The highly disharmonized state of IoT security regulations, however, pulls against that public interest. Moreover, a further doubling down on the current national approaches threatens to worsen the problem. What little compromise in national autonomy this or another consolidated approach might require must be weighed against a more coherent and enforceable scheme where such a scheme produces meaningful security gains for users. To comprehend this need, one should begin by understanding the state of affairs.

The Current State of IoT Risk

The current IoT ecosystem is rife with insecurity. Companies routinely design and develop IoT products with poor cybersecurity practices, including weak default passwords,[3] weak encryption,[4] limited security update mechanisms,[5] and minimal data security processes on devices themselves. Governments, consumers, and other companies then purchase these products and deploy them, often without adequately evaluating or understanding the cybersecurity risk they are assuming. For example, while the US government has worked to develop IoT security considerations for products purchased for federal use, private companies routinely buy and deploy

[3] "Consumer IoT Security Quick Guide: No Universal Default Passwords," IoT Security Foundation, 2020, https://www.iotsecurityfoundation.org/wp-content/uploads/2020/08/IoTSF-Passwords-QG_FINAL.pdf.

[4] Max Eddy, "Majority of IoT Traffic on Corporate Networks Is Insecure, Report Finds," *PCMag*, February 26, 2020, https://www.pcmag.com/news/majority-of-iot-traffic-on-corporate-networks-is-insecure-report-finds.

[5] Xu Zou, "IoT Devices Are Hard to Patch: Here's Why—and How to Deal with Security," TechBeacon, accessed August 17, 2022, https://techbeacon.com/security/iot-devices-are-hard-patch-heres-why-how-deal-security.

insecure IoT products because there is no mandatory IoT security baseline in the United States.[6]

Compromising IoT products is often remarkably easy. IoT products have less computing power, smaller batteries, and smaller amounts of memory than traditional information technology devices like laptops or even smartphones. This makes traditional security software (and its computing and power demands) often impractical in—or less immediately transferrable to—IoT systems. Many IoT botnets (networks of devices infected by malware), such as Mirai and Bashlite, capitalize on this insecurity by seeking to weaponize known vulnerabilities or brute-force access to an IoT product using predefined lists of common passwords. Such passwords may include "123456" or even just "password."[7]

While these errors seem trivial, they quickly lead to material harm. In late 2016, for example, Mirai infected almost 65,000 IoT devices around the world in its first 20 hours, peaking at 600,000 compromised devices.[8] The operators of the Mirai botnet subsequently launched a series of DDoS attacks, including against Dyn, a US-based Domain Name System (DNS) provider and registrar.[9] By taking advantage of security problems in IoT devices, the individuals behind the botnet rendered major websites like PayPal, Twitter, Reddit, GitHub, Amazon, Netflix, and Spotify entirely unavailable to parts of the United States.[10]

Criminals infect IoT products with malware that may use the compromised device to execute DDoS attacks, mine for cryptocurrencies on behalf of the attacker, or hold the device hostage pending a ransom paid to the attackers. In 2018, cybercriminals compromised over 200,000 routers in a cryptojacking campaign. They used the computing power of the compromised routers to mine cryptocurrency.[11] States also turn to compromising IoT products to create covert infrastructure. A May 2022 report by security firm Nisos revealed that the Russian Federal Security Service (FSB) employed a botnet made up of compromised IoT products to fuel social media manipulation operations.[12]

On top of using IoT devices for larger malware operations, hackers can break into IoT products to spy on people's everyday lives. They could see adjustments made to a smart thermostat, questions asked to a smart speaker, and workouts logged on fitness wearables. This kind of spying can be a threat to individuals' privacy and physical safety. In the context of intimate partner violence, abusive individuals may control access to or illicitly access IoT products to spy on and exert control over people, raising serious stalking and physical safety risks.[13] There are also threats that come from strangers. Trend Micro, in a 2019 report, noted that hackers with access to compromised internet-connected cameras sold subscriptions that allowed others to view the illicitly accessed video streams online. The price of the stream depended on what the camera was looking at, with bedrooms, massage parlors, warehouses, and payments desks at retail shops among the priciest and most sought-after.[14] These products can also be launch points from which attackers conduct further malicious activities. Brazilian fraudsters, for instance, are known to use access to compromised routers to change

[6] Gareth Corfield, "Research Finds Consumer-grade IoT Devices Showing up … On Corporate Networks," The Register, October 21, 2021, https://www.theregister.com/2021/10/21/iot_devices_corporate_networks_security_warning/.

[7] Graham Cluley, "These 60 Dumb Passwords Can Hijack over 500,000 IoT Devices into the Mirai Botnet," Graham Cluley, October 10, 2016, https://grahamcluley.com/mirai-botnet-password/.

[8] Manos Antonakakis et al., "Understanding the Mirai Botnet," USENIX 26, August 2017, https://www.usenix.org/system/files/conference/usenixsecurity17/sec17-antonakakis.pdf, 1093, 1098

[9] Antonakakis et al., "Understanding the Mirai Botnet," 1105.

[10] Antonakakis et al., "Understanding the Mirai Botnet," 1105.

[11] "Over 200,000 MikroTik Routers Compromised in Cryptojacking Campaign," Trend Micro, August 03, 2018, https://www.trendmicro.com/vinfo/in/security/news/cybercrime-and-digital-threats/over-200-000-mikrotik-routers-compromised-in-cryptojacking-campaign.

[12] "Fronton: A Botnet for Creation, Command, and Control of Coordinated Inauthentic Behavior," Nisos (blog), May 19, 2022, https://www.nisos.com/blog/fronton-botnet-report/.

[13] Donna Lu, "How Abusers Are Exploiting Smart Home Devices," Vice, October 17, 2019, https://www.vice.com/en/article/d3akpk/smart-home-technology-stalking-harassment.

[14] Stephen Hilt et al., "The Internet of Things in the Cybercrime Underground," Trend Micro, September 10, 2019, https://documents.trendmicro.com/assets/white_papers/wp-the-internet-of-things-in-the-cybercrime-underground.pdf.

the compromised devices' DNS settings to redirect victims to phishing pages for major websites, such as banks and retailers.[15]

IoT Products, Industry Segments, and Their Insecurity

The IoT, on its face, may appear to be a simple concept, but scoping it and understanding the number of systems the IoT touches is more complex. For example, some devices like routers could be "part of" or "separate from" the IoT. There are also questions on the "if, and how" the IoT includes the networks, devices, and products touching it—like IoT sensors linked to outside cloud services to process data, connect to a company's network to enable administrative oversight and control, and connect to the public internet to communicate with application programming interfaces (APIs). For government and industry policies to be effective, scopes must clearly define the products and services they do and do not include.

For instance, EN 303 645 guidance—ETSI's key standard document for IoT security—defines a "consumer IoT device" as a "network-connected (and network-connectable) device that has relationships to associated services and are used by the consumer typically in the home or as electronic wearables."[16] The US National Institute of Standards and Technology (NIST), meanwhile, defines the IoT in NIST SP 1800-16C as "user or industrial devices that are connected to the internet" including "sensors, controllers, and household appliances."[17] This report focuses primarily on the IoT products themselves, and in part the services directly dependent on IoT products or on which IoT products directly depend (e.g., a cloud software program for managing an IoT device network).

The IoT constitutes a massive technology ecosystem with clusters of IoT product design and deployment models, each of which present differentiated cybersecurity risks. Several key examples of industry IoT product segments and some of their security challenges are detailed here, based on their wide deployment, impact on consumers, and touchpoints into other parts of the digital world, whether home Wi-Fi networks or hospital medical systems.

- *Smart Homes:* Numerous companies sell IoT products to serve as thermostats, doorbell cameras, window locks, speakers, and other components of so-called smart homes. Apple offers HomeKit integration, a software framework for configuring, communicating with, and controlling smart home appliances.[18] Resideo offers a number of smart home-style products, for both consumer environments—such as thermostats, humidifiers, security systems, and programmable light switch timers—as well as professional environments—such as UV treatment systems and fire and burglary alarms.[19] Philips sells smart lighting products, and Wink sells smart doorbells.[20] On the software side, companies like Tuya offer IoT management services to automatically control robotic vacuums, smart cameras, smart locks, and other IoT products in the home.[21] Google and Amazon both manufacture and sell smart home IoT products, from home

[15] Pascal Geenens, "IoT Hackers Trick Brazilian Bank Customers into Providing Sensitive Information," Radware (blog), August 10, 2018, https://blog.radware.com/security/2018/08/iot-hackers-trick-brazilian-bank-customers/.

[16] ETSI EN 303 645 – "Cyber Security for Consumer Internet of Things: Baseline Requirements," European Telecommunications Standards Institute (ETSI), (Sophia Antipolis Cedex, France: June 2020), 10, https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.00_30/en_303645v020100v.pdf.

[17] "Internet of Things (IoT)," National Institute of Standards and Technology (NIST), accessed August 17, 2022, https://csrc.nist.gov/glossary/term/internet_of_things_IoT; Mehwish Akram, et al., "NIST Special Publication 1800-16: Securing Web Transactions," NIST, June 2020, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-16.pdf.

[18] Apple Developer, "Developing apps and accessories for the home," Apple, accessed August 25, 2022, https://developer.apple.com/apple-home/.

[19] "All Smart Home Products," Resideo, accessed August 25, 2022, https://www.resideo.com/us/en/products/; "Resideo Pro," Residio, accessed August 25, 2022, https://www.resideo.com/us/en/pro/.

[20] "Philips Hue, Smart Home Lighting Made Brilliant," Philips, accessed August 25, 2022, https://www.philips-hue.com/en-sg; "Ring Video Doorbell," Wink, accessed August 25, 2022, https://www.wink.com/products/ring-video-doorbell/.

[21] "Device Management," Tuya, accessed August 25, 2022, https://www.tuya.com/product/device-management/device-management.

security products to smart speakers.[22] The cybersecurity risks here include spying on individuals in their homes, using IoT products in the home and workplace to break into other systems (e.g., someone's work laptop on their home Wi-Fi), and harnessing numerous compromised smart products to create a botnet and launch DDoS attacks.[23]

- *Networking and Telecommunications Gear:* Traditional internet and telecommunications companies, which supply the devices and some of the infrastructure that fundamentally underpins the internet, are moving more into IoT services and devices. Cisco offers Industrial Wireless solutions that include wireless backhaul, private cellular connectivity, and embedded networking for industrial IoT products.[24] Extreme Networks offers a Defender Adapter service to provide in-line security for vulnerable wired devices.[25] Arista offers a Cognitive Campus service that includes IoT edge connectivity, real-time telemetry, and Spline platforms for connection reliability.[26] The cybersecurity risks here include spying on traffic going across networks, using networking and telecommunications entry points to break into other systems, and degrading or disrupting the flow of network data altogether.
- *Consumer Health Products:* Companies are offering IoT products and services to support the provision of healthcare and medicine. Philips sells fetal and maternal monitors, MR compatible monitors, patient-worn monitors, and other IoT products to monitor vitals.[27] Medtronic sells glucose monitoring and heart monitoring products.[28] Honeywell Life Sciences offers embedded products and safety solutions for hospitals.[29] Dexcom offers a glucose monitoring smart wearable, and ResMed offers a phone-connected product for sleep apnea.[30] The cybersecurity risks here include stealing highly sensitive medical data and manipulating device data or disrupting product operations in ways that physically threaten human life.

Numerous companies, from telecommunications gear manufacturers to medical equipment suppliers, have a stake in security debates about IoT products. Many industries do as well, from home security to industrial manufacturing, and many of their products and services overlap and integrate. Yet, similarities between sector products and their cybersecurity risks do not change the fact that widespread IoT insecurity merits meaningful improvement.

[22] Google Nest Help, "Explore what you can do with Google Nest or Home devices," Google, accessed August 25, 2022, https://support.google.com/googlenest/answer/7130274?hl=en; "Alexa Guard Plus," Amazon, accessed August 25, 2022, https://www.amazon.com/b?ie=UTF8&node=18021383011.

[23] Amazon Web Services, "Security challenges and focus areas," Amazon, accessed August 25, 2022, https://docs.aws.amazon.com/whitepapers/latest/securing-iot-with-aws/security-challenges-and-focus-areas.html; Dave McMillen, "Internet of Threats: IoT Botnets Drive Surge in Network Attacks," Security Intelligence, April 22, 2021, https://securityintelligence.com/posts/internet-of-threats-iot-botnets-network-attacks/.

[24] "Outdoor and Industrial Wireless," Cisco, accessed August 25, 2022, https://www.cisco.com/c/en/us/products/wireless/outdoor-wireless/index.html.

[25] "Defender Adapter," Extreme Networks (data sheet), accessed August 25, 2022, https://cloud.kapostcontent.net/pub/679cf2be-16da-4b6c-91ed-7d504b47a5f1/defender-adapter-data-sheet.

[26] "Cognitive Campus Workspaces," Arista, accessed August 25, 2022, https://www.arista.com/en/solutions/cognitive-campus.

[27] "Maternal and Fetal Monitoring Systems," Philips, accessed August 25, 2022, https://www.usa.philips.com/healthcare/solutions/mother-and-child-care/fetal-maternal-monitoring; "Expression MR400," Philips, accessed August 25, 2022, https://www.usa.philips.com/healthcare/product/HC866185/expression-mr400-mr-patient-monitor; "Wearable Patient Monitoring Systems," Philips, accessed August 25, 2022, https://www.usa.philips.com/healthcare/solutions/patient-monitoring/patient-worn-monitoring.

[28] "Guardian Connect Continuous Glucose Monitoring," Medtronic, accessed August 25, 2022, https://www.medtronicdiabetes.com/products/guardian-connect-continuous-glucose-monitoring-system.

[29] "Healthcare Sensing," Honeywell, accessed August 25, 2022, https://sps.honeywell.com/us/en/products/advanced-sensing-technologies/healthcare-sensing.

[30] "Choose Your Country or Region," Dexcom, accessed August 25, 2022, https://www.dexcom.com/global; "Sleep Apnea – Causes, Symptoms and Treatment," Resmed, accessed August 25, 2022, https://www.resmed.com/en-us/sleep-apnea/.

2. POLICY CHALLENGES TO ADDRESSING IOT RISK

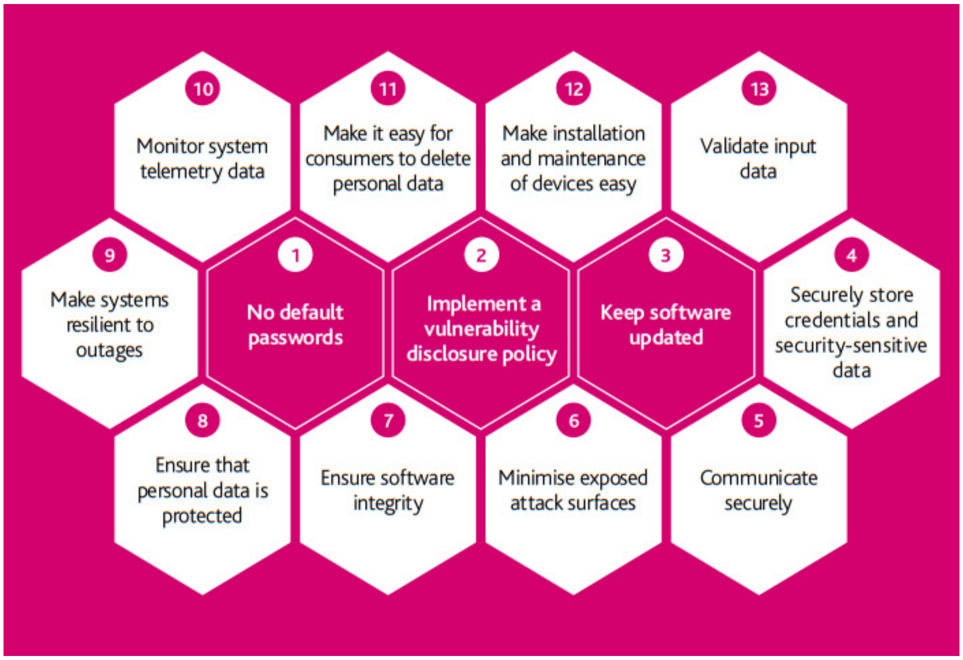
The UK, Singapore, United States, and Australia provide a set of case studies for government approaches to IoT security—due to the maturity of their IoT cybersecurity approaches, the maturity of their overall cyber policy processes, their historical influence on cybersecurity policy in other countries, and the strong precedent for cooperation across all four. There is also fragmentation within the countries' frameworks, where different parts of a country or different government agencies pursue different IoT security policies and processes. The US, for instance, has the Federal Communications Commission (FCC) focused on communications standards for IoT products and the Federal Trade Commission (FTC) focused on the marketing practices of IoT vendors, but has no agency in charge of enforcing IoT security requirements in design.

At least three key themes stand out across these countries. First, state approaches to IoT security have generally moved from voluntary best practices towards direct intervention. Second, state approaches have predominantly manifested in consumer labeling programs and minimum baseline security legislation. And third, states have made the need for international, agreed-upon standards a key design principle of their IoT security efforts though as yet without sufficient uptake or success.

UK: Mandatory Minimum Security Standards

The UK was an early innovator in holistic responses to IoT insecurity. Its Department for Digital, Culture, Media & Sport (DCMS)—which works on digital economy and some broadband and Internet issues—published a Secure by Design report in March 2018, setting out how it aims to "work with industry to address the challenges of insecure consumer IoT."[31] As a result of its report, in October 2018, DCMS, along with the UK National Cyber Security Centre (NCSC) and industry partners, published the "Code of Practice for Consumer Internet of Things (IoT) Security," consisting of "thirteen outcomes-focused guidelines that are considered good practice in IoT security."[32] It aims, as one NCSC official described it, to identify impactful, updatable measures to which a broad coalition could agree[33]—captured in the below principles (Figure 1).

Figure 1: Thirteen Principles of Consumer IoT Security


10
Monitor system telemetry data
11
Make it easy for consumers to delete personal data
12
Make installation and maintenance of devices easy
13
Validate input data
9
Make systems resilient to outages
1
No default passwords
2
Implement a vulnerability disclosure policy
3
Keep software updated
4
Securely store credentials and security-sensitive data
8
Ensure that personal data is protected
7
Ensure software integrity
6
Minimise exposed attack surfaces
5
Communicate securely

SOURCE: UK Department for Digital, Culture, Media & Sport.

[31] "Code of Practice for Consumer IoT Security," United Kingdom Department for Digital, Culture, Media & Sport (DCMS) 2018, https://www.gov.uk/government/publications/code-of-practice-for-consumer-iot-security/code-of-practice-for-consumer-iot-security.

[32] DCMS, "Code of Practice."

[33] PAE interview, United Kingdom National Cyber Security Centre (NCSC), Spring 2022.

The UK was not alone in this endeavor, working in tandem as a member of ETSI to launch ETSI Technical Specification 303 645, the first "globally-applicable industry standard on internet-connected consumer devices."[34] In June 2020, this Technical Specification became formalized as a European standard (EN 303 645), and now serves as a common underlying source for many countries' initiatives.

Despite the initial promise of the Code of Practice, the DCMS found low industry uptake for the guidance and decided to pursue a legislative route. After multiple consultation rounds, the resulting Product Security and Telecommunications Infrastructure (PSTI) Bill was introduced in November 2021, empowering the Secretary of State for DCMS "to specify by regulations security requirements."[35], [36] The new law would require "manufacturers, importers, and distributors to ensure that minimum security requirements are met in relation to consumer connectable products that are available to consumers."[37] Noncompliant firms could face fines up to £10 million or 4 percent of worldwide revenue, and a new regulator—to be delegated following the law's enactment—would also have the ability to enforce recalls or outright product bans.[38] The bill is currently in the Report stage with the House of Lords and would require compliance within twelve months of enactment.

By empowering the DCMS minister to specify security requirements instead of codifying them, the PSTI Bill allows the mandatory baseline requirements to respond to changing circumstances. The current principles outlined by DCMS focus on the "top three" elements of the UK Code of Practice/ETSI EN 303 645: banning default passwords, requiring a vulnerability disclosure process for products, and transparency for consumers on the duration that products will receive security updates. The UK's NCSC views these three measures as having outsize importance, and "will make the most fundamental difference to the vulnerability of consumer connectable products in the UK, are proportionate given the threats, and universally applicable to devices within scope."[39] Cognizant that good security must require organizational action, not just device-level changes at the point of design and manufacture, a DCMS official has highlighted the additional appeal of the framework in allowing requirements placed on economic actors, not just devices. Indeed, two of the three requirements involve organizational changes or activity. The UK's framework allows for the introduction of secondary legislation to build on this baseline over time.

Singapore: IoT Product Labeling

In October 2020, Singapore's Cyber Security Agency (CSA) launched the Cybersecurity Labelling Scheme (CLS), a labeling program for internet-connected devices that describe the level of security included in their design. The CLS aims to help consumers "easily assess the level of security offered and make informed choices in purchasing a device."[40] It also aims to let product manufacturers signal the cybersecurity features of their products—as a senior CSA official put it, "to create the demand" and then "to provide a natural incentive to provide more secure and trusted devices."

The CLS has four levels of additive and progressively demanding security provision tiers (Figure 2). In the first two levels, developers self-certify, and the CSA can audit compliance. In the third and fourth levels, independent laboratories certified by the nongovernmental International Organization for Standardization (ISO) validate products. At the bottom end, products must have security updates and no universal default passwords, while manufacturers must adhere to secure-by-design principles, such as processes and policies for protecting personal data, securely storing security parameters, and conducting threat risk assessments. At the higher end, authorized labs conduct penetration tests against the product and its communications. Labels are valid as long as developers support the product with security updates, for up to a three-year period.

[34] Sophia Antipolis, "ETSI Releases World-leading Consumer IOT Security Standard," news release, European Telecommunication Standards Institute (ETSI), June 30, 2020, https://www.etsi.org/newsroom/press-releases/1789-2020-06-etsi-releases-world-leading-consumer-iot-security-standard.

[35] "The Product Security and Telecommunications Infrastructure (PSTI) Bill – Product security Factsheet," United Kingdom Department for Digital, Culture, Media & Sport (DCMS), November 24, 2021, https://www.gov.uk/guidance/the-product-security-and-telecommunications-infrastructure-psti-bill-product-security-factsheet

[36] "Product Security and Telecommunications Infrastructure Bill Explanatory Notes," UK Parliament, accessed August 17, 2022, https://publications.parliament.uk/pa/bills/cbill/58-02/0199/en/210199en.pdf.

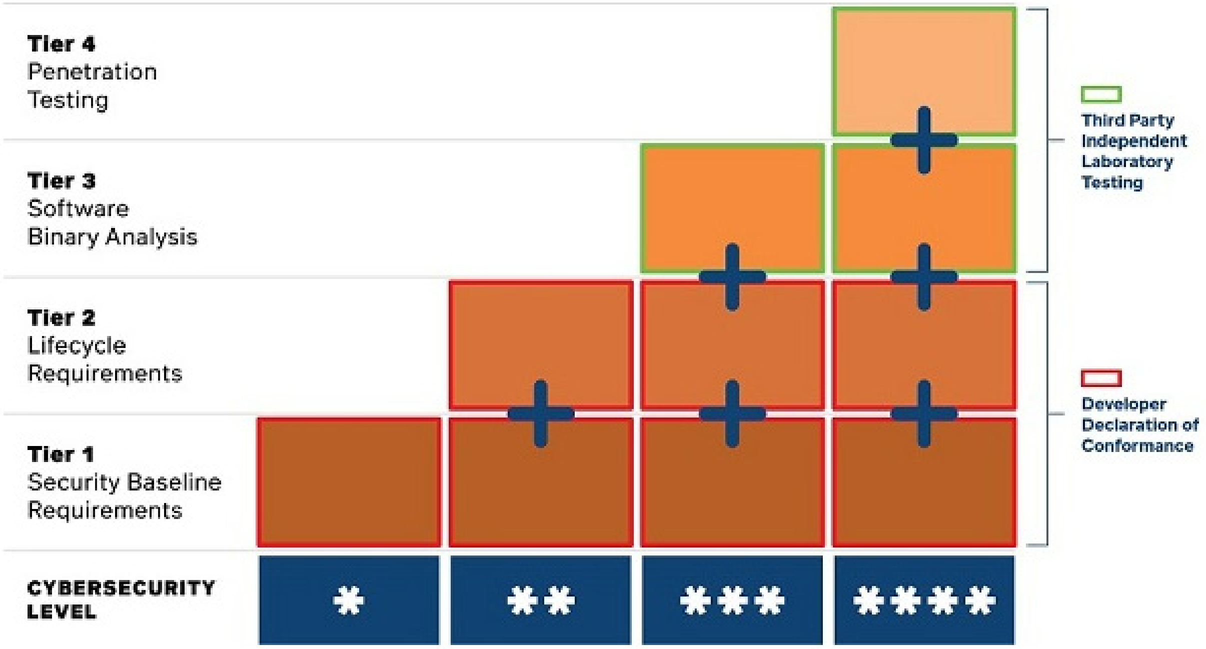
[37] DCMS, "PSTI Product Fact Sheet."

[38] James Coker, "UK Introduces New Cybersecurity Legislation for IoT Devices," *Info Security*, November 24, 2021, https://www.infosecurity-magazine.com/news/uk-cybersecurity-legislation-iot/.

[39] "Regulation of Consumer Connectable Product Cyber Security," RPC-DCMS-4353(2), United Kingdom Department for Digital, Culture, Media & Sport (DCMS), 2021, https://bills.parliament.uk/publications/43916/documents/1025.

[40] Cybersecurity Labelling Scheme (CLS) Updates, Singapore Cyber Security Agency (CSA), 2021, https://www.csa.gov.sg/Programmes/certification-and-labelling-schemes/cybersecurity-labelling-scheme/updates.

Figure 2: Singapore's CLS Four Security Provisions Tiers



SOURCE: Cybersecurity Agency of Singapore.

While the program's terminology slightly differs, the CLS embraces the same principles as ETSI EN 303 645, doing so in a manner that "groups the clauses and spreads them out across four ranked levels."[41] And while the program's higher-tier labels incentivize the adoption of stronger security measures, the Singapore Standards Council concedes that the first-tier labeling requirements "will suffice in staving off [sic] large percentage of attacks encountered on the internet today."[42] Finally, Singapore's CLS shows how a voluntary labeling scheme can work to gradually dial up requirements for products as the market matures. For example, while the CLS is voluntary for most products, new internet routers sold in Singapore must meet the security requirements for the Level 1 label. This "voluntary-mandatory" split can keep evolving over time, both for different product categories as well as specific security measures.

Interviewees at CSA said vendors have reacted positively to the labeling program (e.g., citing the onboarding of major vendors like Google and Asus). As of July 2022, there were 174 certified products, a total that has more than tripled since the start of 2022, and includes diverse items such as smart lights, video doorbells, locks, appliances, routers, and home hubs.[43] Despite these positive signs, it is too soon to tell if the CLS program will be a success, and Singapore must continue to monitor the label's appeal for consumers and firms as well as its broader security impact.

US: State Initiatives & Government Procurement

In the United States, initial action on consumer IoT insecurity began at the state level. The nation's first IoT security law went into effect in January 2020 with California's requirement that manufacturers of smart products sold in the state "equip the device with a reasonable security feature or features." The law explicitly takes aim at universal default passwords, stating that a reasonable security feature could mean "the preprogrammed password is unique to each device manufactured," or "the device contains a security feature that requires a user to generate a new means of authentication before access

[41] Singapore Standards Council, "Technical Reference 91 – Cybersecurity Labelling for Consumer IoT," Enterprise Singapore, 2021, https://www.singaporestandardseshop.sg/Product/SSPdtDetail/41f0e637-22d6-4d05-9de3-c92a53341fe5

[42] Singapore Standards Council, "Technical Reference 91 – Cybersecurity Labelling."

[43] Cybersecurity Labelling Scheme (CLS) Product List, Cyber Security Agency (CSA), 2022, https://www.csa.gov.sg/Programmes/certification-and-labelling-schemes/cybersecurity-labelling-scheme/product-list.

is granted to the device for the first time."[44] California's law—enforced by state attorneys—does not include a private right of action, nor does it put any duties on retailers to ensure that products they sell meet the law's requirements.

Oregon joined California with its House Bill (HB) 2395, which has much of the same text (e.g., the same definition of "reasonable security feature" the same enforcement mechanisms) but limits its scope to only consumer IoT products ("used primarily for personal, family or household purposes").[45] While the two laws may compel companies to adopt better security in all states, it appears that no cases have been brought forward under the law, even though insecure products are doubtlessly still sold in these states.

The United States passed the IoT Cybersecurity Improvement Act into law in December 2020.[46] It requires NIST to develop cybersecurity standards and guidelines for federally owned IoT products, consistent with NIST's understanding of "examples of possible security vulnerabilities" and management of those vulnerabilities.[47], [48] Thus, the law seeks to strengthen the security of IoT products procured by the government and intends to influence the private sector's IoT cybersecurity practices through the federal government's procurement power.[49] The 2020 act also shifts the burden of compliance from product vendors to federal agencies,[50] prohibiting them "[from] procuring or obtain[ing] IoT devices" that an agency's chief information officer deems out of compliance with NIST's standards.[51] Finally, the act requires NIST to review and revise its standards at least every five years to ensure that recommendations are current, allowing for technical flexibility.[52] NIST is empowered to suggest whatever finding it wants, with only vague guidance to consider "secure development" and other high-level cybersecurity items. Figure 3 offers an overview of the act's recommendations.

On May 12, 2021, the Biden administration issued Executive Order (EO) 14028, "Improving the Nation's Cybersecurity." The executive order directed NIST, in consultation with the FTC, to develop cybersecurity criteria for an IoT product labeling program aimed at educating consumers about IoT products' security capabilities.[53] It also tasked NIST with examining how to incentivize IoT manufacturers to get on board with such a program. On February 4, 2022, NIST released its recommended criteria for a consumer IoT labeling scheme.[54] However, NIST has been clear that its aim is to describe the ideal components of a labeling scheme, rather than implement this scheme itself.[55] While EO 14028 may feel a little toothless at the moment, it effectively outlines specific federal cybersecurity goals. Moreover, it demonstrates a will to move beyond federal procurement power as the sole method for influencing the private sector.

Australia: Starting with Voluntary Best Practices

In August 2020, the Australian Department of Home Affairs (DHA) released a voluntary "Code of Practice: Securing the Internet of Things for Consumers" as part of its 2020 cybersecurity strategy. This code of practice highlighted the thirteen principles outlined in ETSI EN 303 645.

Australia's voluntary code of practice did not prove to be a panacea. In March 2021, the Australian government published six months of research on the results of its Code of Practice, saying firms "found it difficult to implement voluntary, principles-based guidance," and many

[44] Senate Bill No. 327, Chapter 886, California Legislative Information, 2018, https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB327.

[45] House Bill 2395, Chapter 193, Oregon State Legislature, 2019, https://olis.oregonlegislature.gov/liz/2019R1/Measures/Overview/HB2395.

[46] IoT Cybersecurity Improvement Act of 2020, Pub. L. No. 116-207 (2020).

[47] IoT Cybersecurity Improvement Act of 2020, Pub. L. No. 116-207 (2020) at §4(a)(1).

[48] Deborah George. "New Federal Law Alert: The Internet of Things (IoT) Cybersecurity Improvement Act of 2020 – IoT Security for Federal Government-Owned Device," *National Law Review*, December 10, 2020, https://www.natlawreview.com/article/new-federal-law-alert-internet-things-iot-cybersecurity-improvement-act-2020-iot.

[49] H.R. 1668 Rep. No. 116-501, Part I (2020), (Proclaiming the purpose of the IoT Cybersecurity Improvement Act of 2020 bill as "to leverage Federal Government procurement power to encourage increased cybersecurity for Internet of Things devices…"), https://www.congress.gov/bill/116th-congress/house-bill/1668/text/rh.

[50] IoT Cybersecurity Improvement Act of 2020, Pub. L. No. 116-207 (2020) at §4(a)(1) & (2)(B)(i)-(iv).

[51] IoT Cybersecurity Improvement Act of 2020, Pub. L. No. 116-207 (2020) at §4(a)(1) & (2)(B)(i)-(iv).

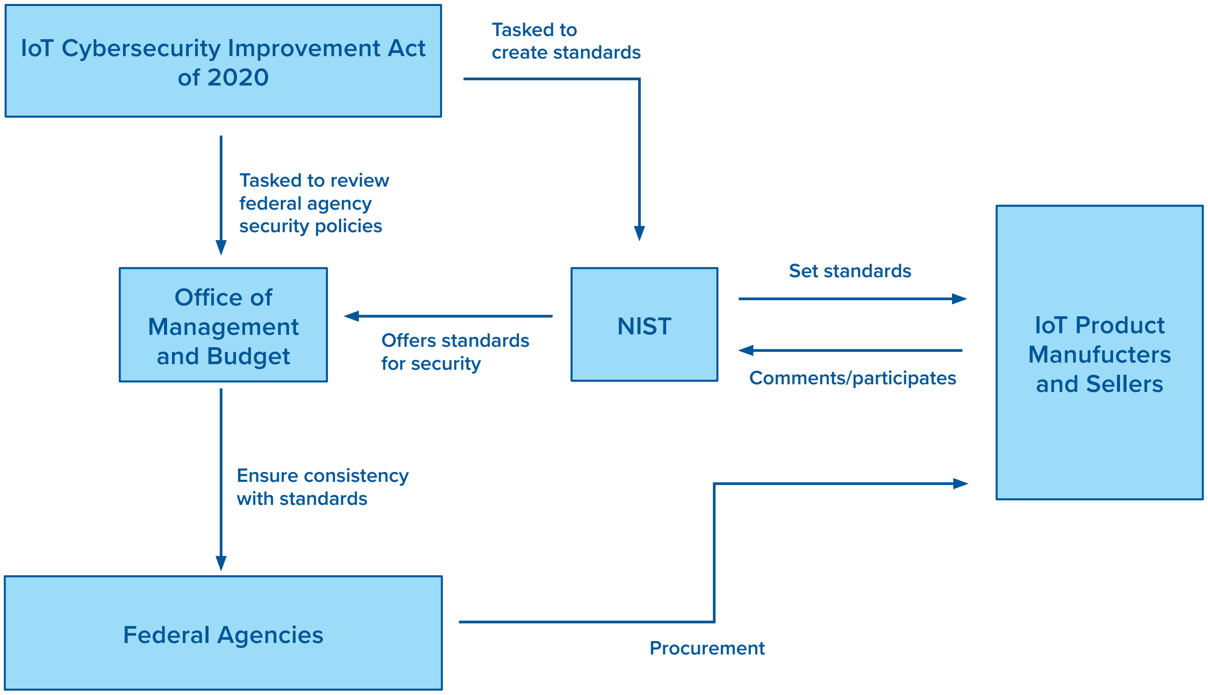
[52] IoT Cybersecurity Improvement Act of 2020, Pub. L. No. 116-207 (2020) at §4(c)(1)(A)-(B).

[53] President Biden,"Executive Order 14028 on Improving the Nation's Cybersecurity," *The White House*, May 12, 2021, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/.

[54] "IoT Product Criteria," National Institute of Standards and Technology (NIST), May 24, 2022, https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity/iot-product-criteria.

[55] "NIST Developed an IoT Label. How Do We Get It onto Shelves?" *New America*, March 1, 2022. https://www.youtube.com/watch?v=ZwDFb3DEkMw.

Figure 3: Overview of the IoT Cybersecurity Improvement Act of 2020


IoT Cybersecurity Improvement Act of 2020
Tasked to create standards
Tasked to review federal agency security policies
Office of Management and Budget
Offers standards for security
NIST
Set standards
Comments/participates
IoT Product Manufucters and Sellers
Ensure consistency with standards
Federal Agencies
Procurement

SOURCE: Liv Rowley for the Atlantic Council.

had still not implemented basic security guidelines like a vulnerability disclosure reporting process.[56] As such, the Australian government appears intent on conducting more direct regulation of its consumer IoT market. In a request for comments that concluded in fall 2021, the DHA solicited public opinion on both a proposed consumer labeling program and a minimum security standards regime.[57]

For the minimum security standards approach, the government proposes to base its requirements on ETSI EN 303 645 and is considering either mandating all 13 guidelines or choosing to focus on just the top three (no default passwords, the existence of vulnerability disclosure programs, and the provision of security updates). The potential regulator within the Australian government is yet to be determined, but it would be empowered to issue fines and other penalties for those who fail to comply.

The potential labeling approaches consider two scenarios. A voluntary "star rating label," such as Singapore's CLS program, basing it on an existing international standard, such as ETSI EN 303 645, and involve some component of self-certification and testing within the framework of Australian consumer law's protection against fraudulent claims. Alternatively, a mandatory "expiry date label" would indicate the period over which the product will receive critical security updates. This second option received a higher recommendation from the government. Minimum security standards could complement either of these approaches.

Industry: Certification Models and Security Standards

Companies have also advanced numerous security approaches. Common industry approaches to IoT security include secure endpoints and stringent encryption requirements for third-party applications, hardware-based security, and the formalization of vulnerability and software communications protocols. The industry verticals for smart homes, networking and telecommunications, and consumer healthcare (recognizing there is overlap and integration between these verticals) see varying implementations of these measures.

For example, the ioXt Alliance, which is composed of dozens of product manufacturers and vendors as well

[56] "Voluntary Code of Practice: Securing the Internet of Things for Consumers," Australian Department of Home Affairs (DHA), [updated March 22, 2022], https://www.homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers/code-of-practice.

[57] "Strengthening Australia's cyber security regulations and incentives," Australian Department of Home Affairs (DHA),[updated March 22, 2022], https://www.homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers/cyber-security-regulations-incentives.

as major software companies, offers self-certified and third-party-validated certification for IoT products. Its five compliance tests cover everything from Android to smart speaker device profiles, measured against eight principles: no universal default passwords, secured interfaces, proven cryptography, security by default, verified software, automatic security updates, vulnerability reporting program, and security expiration date.[58] The overall certification process has five steps:

1. Join the ioXt Alliance and register for certification;

2. Select one of the five base profiles for testing, and then opt to self-certify or use one of the ioXt's approved laboratories (currently, Bureau Veritas, SGS Brightsight, DEKRA, NCC Group, NowSecure, Onward Security, or Bishop Fox[59]);

3. Upload production information and test results to the ioXt portal;

4. ioXt reviews the submissions and approves or rejects certification—with approved submitters receiving "the ioXt SmartCert" for their product; and

5. "Stay certified with ongoing verification and insights," like IoT regulatory updates through the Alliance.[60]

The Alliance's membership includes companies like IBM, Google, Facebook, Silicon Labs, Logitech, Honeywell, Avast, Asus, Motorola, and Lenovo; other associations like the Consumer Technology Association (CTA) and the Internet Infrastructure Coalition; and non-industry organizations like Consumer Reports. Even the UK's DCMS is an Alliance member.[61] While the membership roster certainly does not cover every IoT product manufacturer or vendor in the United States (where many of its members are based), it does have global representation. It also certified 245 percent more products and membership increased 63 percent in 2021 compared to 2020.[62]

The IoT Security Foundation, a global nonprofit representing many appliance manufacturers, recommends a framework composed of a few hundred security standards for organizations—spanning management governance, engineering, secure networks and applications, and supply chain.[63] Its members include smaller product manufacturers as well as larger companies like Honeywell, Huawei, and Arm, plus many more nongovernmental organizations, like academic institutions, than the ioXt Alliance.[64] The framework has three different audiences: (1) managers, (2) developers and engineers, and logistics and manufacturing staff, and (3) supply chain managers.[65] While its membership is not as large as that of the ioXt Alliance, the IoT Security Foundation does have global representation as well, such as the University of Southampton, Huawei, the University of Oxford Department of Computer Science, and Eurofins Digital Testing in France.[66]

The Open Web Application Security Project® (OWASP) is an open-source community effort that provides IoT security standards tailored to three threat models—attacks only against software, attacks only against hardware, and situations where compromise must be avoided at all costs (e.g., medical products, connected vehicles, due to highly sensitive data, etc.).[67] OWASP then specifies several dozen security standards based on these threat models, such as standards for bootloader vs. OS configurations vs. Linux.[68] OWASP is a nonprofit foundation with over 250 local chapters worldwide and tens of thousands of members, and it runs training conferences and other events to bring together experts from industry, academia, and civil society focused on software development and security.[69] Its capacity to drive change on IoT security is considerably different from the previous two coalitions—for instance,

[58] "Get ioXt Certified," ioXt, accessed August 17, 2022, https://www.ioxtalliance.org/get-ioxt-certified.

[59] "Authorized Labs," ioXt, accessed August 17, 2022, https://www.ioxtalliance.org/authorized-labs.

[60] "Certifying Your Product," ioXt, accessed August 17, 2022, https://www.ioxtalliance.org/certifying-your-device

[61] "The Global Standard for IoT Security," ioXt, accessed August 17, 2022, https://www.ioxtalliance.org.

[62] "ioXt Alliance Closes Record Year of Membership Growth and Certifications," Businesswire, January 19, 2022, https://www.businesswire.com/news/home/20220119005139/en/ioXt-Alliance-Closes-Record-Year-of-Membership-Growth-and-Certifications.

[63] "IoT Security Assurance Framework," IoT Security Foundation, November 2021,https://www.iotsecurityfoundation.org/wp-content/uploads/2021/11/IoTSF-IoT-Security-Assurance-Framework-Release-3.0-Nov-2021-1.pdf.

[64] "IoT Security Foundation Members," IoT Security Foundation, accessed August 17, 2022, https://www.iotsecurityfoundation.org/our-members/.

[65] IoT Security Foundation, "IoT Security Assurance Framework."

[66] IoT Security Foundation, "IoT Security Foundation Members"; "Eurofins Digital Testing Your Trusted Partner in Quality," Eurofins, accessed August 17, 2022, https://www.eurofins-digitaltesting.com.

[67] "OWASP IoT Security Verification Standard," Open Web Application Security Project® (OWASP), accessed August 17, 2022, https://owasp.org/www-project-iot-security-verification-standard/; "IoT Security Verification Standard (ISVS)," GitHub, accessed August 17, 2022, https://github.com/OWASP/IoT-Security-Verification-Standard-ISVS.

[68] "IoT Security Verification Standard (ISVS)," GitHub, accessed August 17, 2022, https://github.com/OWASP/IoT-Security-Verification-Standard-ISVS.

[69] "About the OWASP Foundation," Open Web Application Security Project® (OWASP), accessed August 17, 2022, https://owasp.org/about/.

the OWASP community cannot marshal the marketing and lobbying power held by members of the ioXt Alliance or the IoT Security Foundation. However, OWASP draws on its tens of thousands of members around the world and leverages different forms of engagement than the other coalitions. The IoT Security Foundation, for instance, does not run events at the same scale as OWASP.

The GSM Association, an industry group for mobile network operators, has hundreds of industry members—from Amazon to Coinbase to Audi—and has numerous guidance documents for IoT security.[70] For example, it has security considerations ranging from having password policies protect against hard-coded or default passwords (CLP12_6.11.1.5) to having a process for decommissioning endpoint devices (CLP13_8.10.1).[71]

The CTA, a standards and trade organization with over 1,000 company members, runs an IoT Working Group that supports consumer IoT development. Included in those efforts is educating consumers about IoT security best practices and improving the security of IoT products.[72] The CTA has multiple labeling schemes under development around IoT products, focused on consumer-facing product security descriptions managed through an accreditation system.[73] The CTA, in fact, submitted a position paper to NIST in 2021 that described its vision for a cybersecurity labeling system for software and IoT devices—noting that labels should reflect the consensus industry standards, avoid marketplace fragmentation, and look to risk assessment as much as specific security capabilities, among others.[74] It also has global reach, with Cisco, Google, Panasonic, Samsung, Walmart, Alibaba, Nvidia, and ADT among its members.[75]

The Connectivity Standards Alliance (CSA), which develops and certifies IoT technology standards, has a number of documents and efforts focused on security. For example, the CSA website contains numerous developer resources on IoT security, from security and privacy guidance on the CSA-developed IP-based protocol Matter to documentation around Zigbee, the low-latency communication specification.[76] The CSA's product security working group is underway, developing security standards for IoT devices and exploring security options around labeling and it has a recently started IoT privacy effort, as well. Both of these endeavors focus on consumer-facing security considerations (meanwhile, other CTA efforts focus on less consumer-facing aspects of IoT product security). The CSA has nearly 300 participant companies and dozens of sponsors around the world, and it also has hundreds of corporate adopters—ranging from large retailers like Amazon to device and component developers like Arm, Silicon Labs, Schneider Electric, LG, Huawei, and Google.[77]

Individual companies have also provided their own guidance, such as Google's Cloud IoT Core "device security" guidelines,[78] Microsoft's Edge Secured-core criteria,[79] and Arm's Platform Security Architecture for the IoT.[80] Each emphasizes different threat models and targets different stakeholders in the IoT process, from product engineers to those in management at product manufacturers.

While beneficial, these approaches in the aggregate present a fragmented industry approach to IoT security. Governments looking to industry standards as a reference point find numerous, very different options; for instance, while the ioXt Alliance's security approach emphasizes testing against specific device profiles, the OWASP approach emphasizes different kinds of threat models that could, hypothetically, apply across device profiles. There are also implementation differences: the ioXt Alliance points to independent, third-party testing and evaluation, whereas OWASP offers a list of standards that organizations can pair to a particular threat model. Some yet (like the ioXt Alliance) create new, IoT security-specific approaches, and others (like Arm) offer rough replicas of their overall cybersecurity guidance, with some tailoring to IoT.

[70] GSM Association, "GSMA IoT Security Guidelines and Assessment," Groupe Speciale Mobile, or GSMA, accessed August, 4, 2022, https://www.gsma.com/iot/iot-security/iot-security-guidelines/.

[71] GSM Association, "IoT Security Assessment Checklist," Groupe Speciale Mobile, or GSMA, accessed August 4, 2022, https://www.gsma.com/iot/iot-security-assessment/.

[72] CTA, "IoT Working Group," Consumer Technology Association, accessed September 22, 2022, https://www.cta.tech/Membership/Member-Groups/IoT-Working-Group#:~:text=The%20Consumer%20Technology%20Association%20(CTA,education%2C%20standards%20and%20policy%20efforts.

[73] CTA, "IoT Working Group," Consumer Technology Association.

[74] CTA, "Cybersecurity Labeling, Conformity Assessment and Self-Attestation (CTA)," Consumer Technology Association, accessed September 22, 2022, https://www.nist.gov/system/files/documents/2021/09/03/CTA%20Position%20Paper%20on%20Cybersecurity%20Label%20Considerations%20Final.pdf.

[75] CTA, "Member Directory," Consumer Technology Association, accessed September 22, 2022, https://members.cta.tech/cta-member-directory?_ga=2.13576244.208474513.1663814734-503620203.1663814734&reload=timezone

[76] Connectivity Standards Alliance, accessed September 22, 2022, https://csa-iot.org/.

[77] CSA, "Community, The Power of Membership," Connectivity Standards Alliance, accessed September 22, 2022, https://csa-iot.org/members/.

[78] "Device security," Google Cloud, accessed August 17, 2022,https://cloud.google.com/iot/docs/concepts/device-security.

[79] "Azure Certified Device – Edge Secured-core," Microsoft, August 11, 2022, https://docs.microsoft.com/en-us/azure/certification/program-requirements-edge-secured-core?pivots=platform-linux.

[80] "Architecture Security Features," Arm, accessed August 17, 2022, https://developer.arm.com/architectures/architecture-security-features/platform-security.

Summarizing Challenges

The current government approaches towards IoT security present many challenges—and have many gaps and shortfalls. This matters across the United States, Singapore, Australia, the UK, and many other governments, because industry has failed to appropriately invest in IoT security, leaving governments to step in. Simultaneously, some states are leading aggressively on securing IoT while others appear willing, on a structural level, to cede that leadership to industry (or to not act at all). Australia, for example, has put forward an IoT security framework but has long delayed the publication of specific guidance.

Industry organizations have pursued a range of IoT security approaches across labeling, certification, minimum standards, and best practices. This guidance also varies across industry verticals—for instance, given embedded IoT healthcare devices face many more regulatory security requirements than smart speakers. All these initiatives represent a substantial effort and reflect years of work from individuals in the security community—yet challenges (Table 1) around enforcement and implementation leave room for greater cohesion to tie security actions to particular parts of the product lifecycle.

On the private sector side, ambiguous requirements and policy goals,[81] diverging processes and regulatory requirements across jurisdictions, and duplicative certification schemes all hinder private-sector efforts to boost IoT security. And on the user side, individuals are grappling with little to no information to select more secure products, bad security outcomes and insecurity, and harmful knock-on effects from IoT insecurity that harm others in society and using the internet.

State IoT Security Challenges

State IoT security policies are fragmented across jurisdictions. While the United States, UK, Singapore, and Australia (as well as the EU bloc) have generally moved from a voluntary best practices approach toward a mandatory approach, the states' policies do not necessarily integrate well with one another. Each country has different specific cybersecurity best practices and places different levels of regulatory requirements on companies. This state-to-state fragmentation makes it more difficult for governments to agree on IoT security goals and operationalize IoT security cooperation—impeding a multinational approach to systemic risk.

Further, when states work to increase cooperation, there is a question of selectivity and exclusion: the ten countries with the most infected devices in the 2016 Mirai botnet were primarily in South America and Southeast Asia.[82] Meanwhile, most high-resourced countries principally focus on IoT security collaboration with one another (e.g., UK-Singapore IoT security collaboration), not on building IoT security capacity in lower-resourced countries. The latter does happen—for example, Singapore and the Netherlands have engaged the nonprofit, multistakeholder Global Forum on Cyber Expertise on global

Table 1: Challenges with Current IoT Security Models

Challenges for State	Challenges for Private Sector	Challenges for Users
Fragmented approach across jurisdictions. Fragmented/gap-filled approach *within* jurisdictions.	Ambiguous requirements and policy goals. Diverging processes and regulatory requirements across jurisdictions. Duplicative certification schemes, including cost, time consumption, and mix of binary/tiered/descriptive certifications.	Little to no information to select more secure products. Bad security outcomes and insecurity. Harmful knock-on effects to others in society and using the internet.

SOURCE: Justin Sherman for the Atlantic Council.

[81] To the reader: For instance, the ioXt Alliance has clear requirements and is clear about its desired means of improving IoT cybersecurity—"multi-stakeholder, international, harmonized, and standardized security and privacy requirements, product compliance programs, and public transparency of those requirements and programs"—but is not clear about its policy goals beyond general references to improving IoT cybersecurity, see: https://www.ioxtalliance.org/about-ioxt.

[82] Antonakakis et al., "Understanding the Mirai Botnet," 1105.

IoT security issues. Nevertheless, collaboration remains primarily among higher-resourced and higher-capacity states.[83]

Thus, one set of countries debate solutions while excluding a bevy of impacted stakeholders from the discussion. In doing so, higher-resourced countries may miss important points about their IoT frameworks' applicability. Notably, cultural contexts greatly matter alongside technical considerations when weighing country adoption, and IoT product reliability may be just as important if not more so than cybersecurity per se in a development context.[84] In fact, for many countries, increased reliance on information and communication technologies without proper reliability can very well yield suboptimal development outcomes.[85] For example, while other governments (e.g., Singapore, Australia) reference the UK's IoT security recommendations, some of the UK standards may require too much investment for lower-resourced states and focus less on reliability per se than security.

Furthermore, regulatory approaches *within* countries may still be fragmented and leave gaps. For example, in the United States the FCC regulates IoT products' network connectivity, and the FTC regulates the marketing practices of IoT products.[86] The FCC has broad authority to regulate product manufacturers and sellers. On the flip side, the FTC's authority mainly concerns consumer protection to ensure IoT product sellers are not being deceptive.[87] However, this still leaves gaps, such as not incentivizing security requirements at the device manufacturing stage and leaving national laws to govern IoT cybersecurity for federal agencies, while mostly standards and voluntary guidelines guide the private sector.[88] In Australia, to give another example, the state's "privacy, consumer, and corporations laws were not originally intended to address cybersecurity," leaving the national government trying to make do with a patchwork of laws to address cybersecurity.[89] Country-internal fragmentation, in total, leaves policy and regulatory gaps in promoting IoT security, forces the government to grapple with an ill-formed patchwork of authorities and procedures, and raises costs and increases confusion for businesses and users—especially when different labels are in play.

Private Sector IoT Security Challenges

Many IoT security approaches in practice have ambiguous requirements and policy goals that make it difficult for the private sector to both understand and implement the government's vision—and difficult for the state to require or incentivize the private sector to change. Take government procurement requirements, whose aim can be unclear. One aim could be the use of procurement to directly secure specific products, such as by requiring the military to only buy IoT products with a higher cybersecurity bar. Another possibility is using procurement to signal best practices to industry, such as requiring compliance with NIST's cybersecurity framework—mandatory for US federal agencies and which more than 30 percent of US organizations have voluntarily adopted.[90] And another possibility is not just signaling best practices but incentivizing companies broadly, even those not doing federal contracting, to increase their own product security. As one standards body expert put it, "if the government only buys products meeting certain standards, that sets a bar for the private sector."[91]

While the security approach may be similar or identical in each case, there are different policy goals in play that may not be articulated (even if they are not mutually exclusive). If most IoT vendors are not government contractors, the use of federal procurement requirements to secure the broader ecosystem may fail. Danielle Kriz, the senior director of global policy at Palo Alto Networks, argued that government procurement on its own isn't enough to result in full-scale IoT security.[92] Using procurement to signal to the broader market could also produce

[83] "International IoT Security Initiative," Global Forum on Cyber Expertise (GFCE), accessed April 6, 2022, https://thegfce.org/initiatives/international-iot-security-initiative/.

[84] *Harnessing the Internet of Things for Global Development*, (Geneva: International Telecommunication Union, 2015), 7, https://www.itu.int/en/action/broadband/Documents/Harnessing-IoT-Global-Development.pdf.

[85] Robert Morgus, *Securing Digital Dividends: Mainstreaming Cybersecurity in International Development* (Washington, D.C.: New America, April 2018), 38, https://www.newamerica.org/cybersecurity-initiative/reports/securing-digital-dividends/.

[86] Nima Agah, "Segmenting Networks and De-segmenting Laws: Synthesizing Domestic Internet of Things Cybersecurity Regulation," (Durham, NC: Duke University School of Law, 2022), 8–12.

[87] Agah, 8–12.

[88] Efrat Daskal, "Establishing standards for IoT devices: Recent examples," Diplo (blog), December 16, 2020, https://www.diplomacy.edu/blog/establishing-standards-for-iot-devices-recent-examples/.

[89] DHA, "Strengthening Australia's Cyber Security Regulations and Incentives."

[90] US National Institute of Standards and Technology , "Cybersecurity "Rosetta Stone" Celebrates Two Years of Success," National Institute of Standards and Technology, accessed September 22, 2022, https://www.nist.gov/news-events/news/2016/02/cybersecurity-rosetta-stone-celebrates-two-years-success.

[91] US National Institute of Standards and Technology, "Cybersecurity "Rosetta Stone" Celebrates Two Years of Success."

[92] Danielle Kriz, "Governments Must Promote Network-Level IoT Security at Scale," Palo Alto Networks, December 8, 2021, https://www.paloaltonetworks.com/blog/2021/12/network-level-iot-security/.

product fragmentation. David Hoffman, a Duke University professor of cybersecurity policy, argued that if you make the standards too robust, you could create a situation where there is a profit incentive for contractors to sell two different products. One for government and one for the private sector.[93] Further, if introducing a procurement requirement is meant to signal a coming wave of incentives around that set of security requirements, governments should note that—so industry can begin to get on board.

Differences in cybersecurity and IoT security processes, levels of maturity, and regulatory requirements across jurisdictions likewise complicate the private sector's implementation of IoT security approaches. When a country's internal approach to IoT security is fragmented, it becomes harder to coordinate with the private sector as well as other countries—because there is no clear and cohesive national approach. Companies, for their part, often find themselves caught between multiple competing, if not contradictory, IoT cybersecurity regimes. This increases industry confusion about IoT security best practices (particularly for businesses with less institutionalized cybersecurity capacity) and may force IoT manufacturers and vendors to tailor-make products to meet specific, varied regulatory requirements (discussed in the next section). Disjointed IoT security standards also raise the costs of government interaction for companies, especially for smaller players with less budget and in-house governmental relations capacity. Vendors and manufacturers that have more money and resources could therefore have an even more outsized ability to influence the security conversation.

For industry, certification schemes also introduce many challenges. The current IoT security certification approach emphasizes independent, third-party product certification—time-consuming and costly (sometimes in the tens of thousands of dollars)—which may be outright prohibitive for smaller manufacturers and vendors. This approach often excludes lower-cost approaches that could work simultaneously, like self-certification to a lower bar of standards. Certification schemes are also binary, tiered, and descriptive; there is no unified approach for companies to implement and understand. For example, Singapore's CLS has four progressively demanding security level provision tiers (see Figure 2): security baseline requirements (Tier 1), lifecycle requirements (Tier 2), software binary analysis (Tier 3), and penetration testing (Tier 4).[94] Others, however, such as many industry certification schemes, are binary, either certifying a product as "secure" under their definition or not doing so at all.

User IoT Security Challenges

The current approach also presents challenges for users. An Ipsos MORI survey in Australia, Canada, France, Japan, the UK, and the United States found that consumers overwhelmingly think that "connected device manufacturers should comply with legal privacy and security standards" (88 percent), "manufacturers should only produce connected devices that protect privacy and security" (81 percent), and "retailers should ensure the connected devices they sell have good privacy and security standards" (80 percent).[95] A majority of those that own connected devices (63 percent) "think they are creepy."[96] Despite these findings, by and large, users continue to purchase insecure IoT products.

Currently, manufacturers and vendors provide users with little to no information to select more secure products. Where labeling and/or certification schemes do exist, they expect that buyers have a fair knowledge of IoT security and will make purchasing decisions based off that knowledge. This user knowledge assumption is faulty, as all countries surveyed in this report are far from sufficiently educating the public on cybersecurity issues. And in the context of a corporate buyer of IoT products, there is no guarantee many organizations purchasing IoT products have deep, in-house capacity around IoT cybersecurity practices, either.

The current approach also leaves users, and the IoT ecosystem in general, with bad security outcomes and insecurity. Many manufacturers and vendors underinvest in cybersecurity and might not even have any kind of robust cybersecurity processes in place in their organization. This manifests itself in IoT products riddled with bad security practices, like default passwords and weak encryption, which leave products, users, and connected systems vulnerable to data theft and much worse. Merely encouraging organizations to adopt voluntary standards (that some organizations may not even know about) does not widely improve IoT security outcomes, either. Further, the labeling and certification schemes that do exist in some jurisdictions are often expensive—and if manufacturers and vendors choose not to absorb the costs themselves, then they will charge consumers higher prices for IoT products.

[93] David Hoffman, Interview with report author, April 6, 2022.

[94] Cyber Security Agency, "CSA | Cybersecurity Labelling Scheme - For Manufacturers," Accessed September 22, 2022, https://www.csa.gov.sg/Programmes/certification-and-labelling-schemes/cybersecurity-labelling-scheme/for-manufacturers.

[95] *The Trust Opportunity: Exploring Consumer Attitudes to the Internet of Things*, Internet Society and Consumers International, May 1, 2019, https://www.internetsociety.org/resources/doc/2019/trust-opportunity-exploring-consumer-attitudes-to-iot/.

[96] Internet Society and Consumers International, *The Trust Opportunity*.

Even if companies wanted to invest and buyers had all this knowledge, the current approach would still negatively impact users, the broader internet ecosystem, and other involved individuals. Given the “paradox of choice,” where increasing the number of options available to someone can make it harder to reach a decision, providing users with many different labels and certifications may do the same. The lack of a unified labeling scheme also makes it difficult for consumers to compare labels (binary versus tiered versus descriptive), and the lack of a single global IoT cybersecurity certification means buyers may not even be able to compare IoT security attestations at all. Moreover, there is little indication that introducing labeling and/or certification would necessarily cause a buyer to look anywhere beyond the price tag. And in the narrow cases where manufacturers or vendors provide labels and certification information to buyers, many users only see that information when the product is already unpacked and undergoing setup in their home or work environment.

Overall, current IoT security approaches still place a heavy security burden on individuals, rather than systematically mandating and incentivizing product manufacturers and vendors to consider and build in security from the outset. As one DCMS official described it, labels may be attractive because they can avoid the bureaucracy of legislation—yet they still expect consumers to move the security needle.

Addressing these challenges should not devolve into championing one national approach over another. The need for harmonization in specific controls is real, and this need extends to control philosophies and enforcement schemes. The section below synthesizes these previous approaches into a single framework based on the general lifecycle of IoT products as a basis for a path forward.

3. CREATING A SYNTHESIZED FRAMEWORK

There is no shortage of IoT security frameworks. As noted in the last section, government agencies, private companies, industry organizations, and civil society groups around the world have developed and published a range of IoT security policy frameworks, design best practices, and security certification schemes. This represents a substantial body of work on IoT security, yet there is more to be done—and its range creates complexity heedless of industry cries for coherence and presents a meaningful obstacle to international coordination.

Rather than address each of the four jurisdictions of interest (US, UK, Australia, Singapore) in isolation, this section presents a consolidated framework with existing security regulations, standards, and guidance from all four countries.

The framework's first goal is to reduce fragmentation between policy approaches by highlighting their contributions and limitations. Operating in multiple jurisdictions with different IoT security regimes can drive up product development and legal compliance costs, disincentivize companies from investing in security or widely selling their products, and even create scenarios where companies must tailor-make IoT products to sell in different countries. Reducing fragmentation addresses these cost issues. It also empowers IoT product users, by giving companies and individuals a clearer set of tradeoffs and information rather than numerous, different stamps of security approval from different places. Lastly, reducing fragmentation helps policymakers forge cooperation internationally and cover the entire IoT security landscape at home.

The framework's second goal is to better situate technical and process guidance into cybersecurity policy. As previously discussed, some government requirements and guidance on IoT security lack detail and have ambiguous policy goals, which impede the private sector's progress on better implementing IoT product security. Integrating technical and process details into government policy can help the private sector, especially companies with limited cybersecurity knowledge and capacity, operationalize higher-level IoT security objectives. It would also help governments identify flaws in their own IoT security approaches; for example, an overemphasis on certifications' policy value has come at the expense of looking at the certification process—which for many organizations is a time-consuming, costly endeavor.

Table 2: Synthesized IoT Security Framework

Phase	Design	Development	Sale & Setup	Maintenance	Sunsetting
Security Action and Policy Options	Following voluntary and/or mandatory technical standards (e.g., encryption). Following voluntary and/or mandatory best practices (e.g., no default passwords). Employing best practice security design principles. Building in functionality that allows obsolete products to continue to operate without an internet connection.	Employing voluntary and/or mandatory technical standards (e.g., encryption). Employing voluntary and/or mandatory best practices (e.g., no default passwords). Tailoring additional security requirements based on risk profile. Implementing mechanisms for regularly updating software.	Implementing vulnerability disclosure policies and processes. Employing labeling schemes. Getting products security-certified. Publishing an end-of-life policy for security updates.	Maintaining vulnerability disclosure policies and processes. Issuing regular security updates. Updating labeling schemes in line with security updates and disclosed vulnerabilities. Updating certifications in line with security updates and disclosed vulnerabilities.	Offering device trade-in incentives. Notifying end users when devices will no longer receive security updates.

SOURCE: Liv Rowley and Justin Sherman for the Atlantic Council.

Table 2 presents a synthesized IoT cybersecurity framework—mapping at what stages of the IoT lifecycle various IoT security actions and policies could be applied. This leads to a discussion in this section of how existing government IoT security approaches have enforced, incentivized, or guided these measures. It then leads to the recommendations section, which discusses ways in which governments can better select from these security action options and appropriately enforce, incentivize, or guide them to achieve better cybersecurity across the IoT ecosystem.

Overwhelmingly, this framework highlights that the IoT security approaches in the countries studied focus on the design, development, and sale, and setup phases of the IoT lifecycle, with significant gaps in security actions and policies for the maintenance and sunsetting phases of an IoT product's lifespan.

Cybersecurity decisions at each lifecycle phase help determine a product's ultimate security (Figure 4).

Design decisions frame how IoT products are ultimately architected, and they can include or exclude certain cybersecurity considerations from the outset. Security action and policy options at this level include following voluntary and/or mandatory technical standards, following voluntary and/or mandatory best practices, and employing best practice security design principles.

Development decisions begin to put those design ideas into practice, and they impact how higher-level ideas and principles are operationally employed into the creation of products. They also present an opportunity for IoT product manufacturers to tailor additional security requirements based on their product's risk profile—for instance, adding in extra controls on top of voluntary, minimum best practices for products used in safety-sensitive or critical infrastructure settings.

Sale and setup decisions focus on IoT products going on the shelf and getting configured in their use environment, and they impact the cybersecurity of those products when first activated. Security action and policy options at this level include implementing vulnerability disclosure policies and processes, implementing mechanisms for regularly updating software, employing labeling schemes, and getting products security-certified.

Maintenance decisions focus on IoT products that have already been configured and deployed, and they impact the security of those products for the rest of their lifetime. The security action and policy options at this level include maintaining vulnerability disclosure policies and processes, issuing regular security updates, updating labeling schemes in line with software security updates and disclosed vulnerabilities, and updating certifications in line with software updates and disclosed vulnerabilities.

And finally, *sunsetting* decisions pertain to the end of a product lifecycle—such as when a vendor stops providing security updates—and how product vendors and users should communicate about, prepare for, and navigate the process of retiring an IoT product.[97]

When applied to the United States, the UK, Australia, and Singapore, the framework shows that most country IoT security approaches concentrate on the earlier parts of the IoT product lifecycle. The *design*, *development*, and *sale and setup* phases are heavily covered. In the United States, existing NIST publications that provide guidance on security-by-design (like NIST SP 800-160) are applicable to IoT.[98] The UK's PSTI Bill, introduced in November 2021 and not yet passed, would require "manufacturers, importers, and distributors to ensure that minimum security requirements are met in relation to consumer connectable products that are available to consumers."[99] The provisions leverage recommendations in the UK Code of Practice/ETSI EN 303 645: banning default passwords, requiring vulnerability disclosure processes for products, and providing transparency for consumers on the duration that products will receive security updates.[100] Nonetheless, there are still gaps; the UK PSTI Bill focuses more on design, development, and sale and setup.[101]

Design and *development* guidance often overlap in the four countries. The Australian government's Code of Practice on securing the IoT for consumers uses the 13 principles laid out by the UK and ETSI, including not using default passwords, implementing a vulnerability

[97] To the reader, it is important to note that users of IoT products must also play a role in ensuring device security. For instance, it is not enough for vendors to make patches; consumers must be sure to apply said patches.

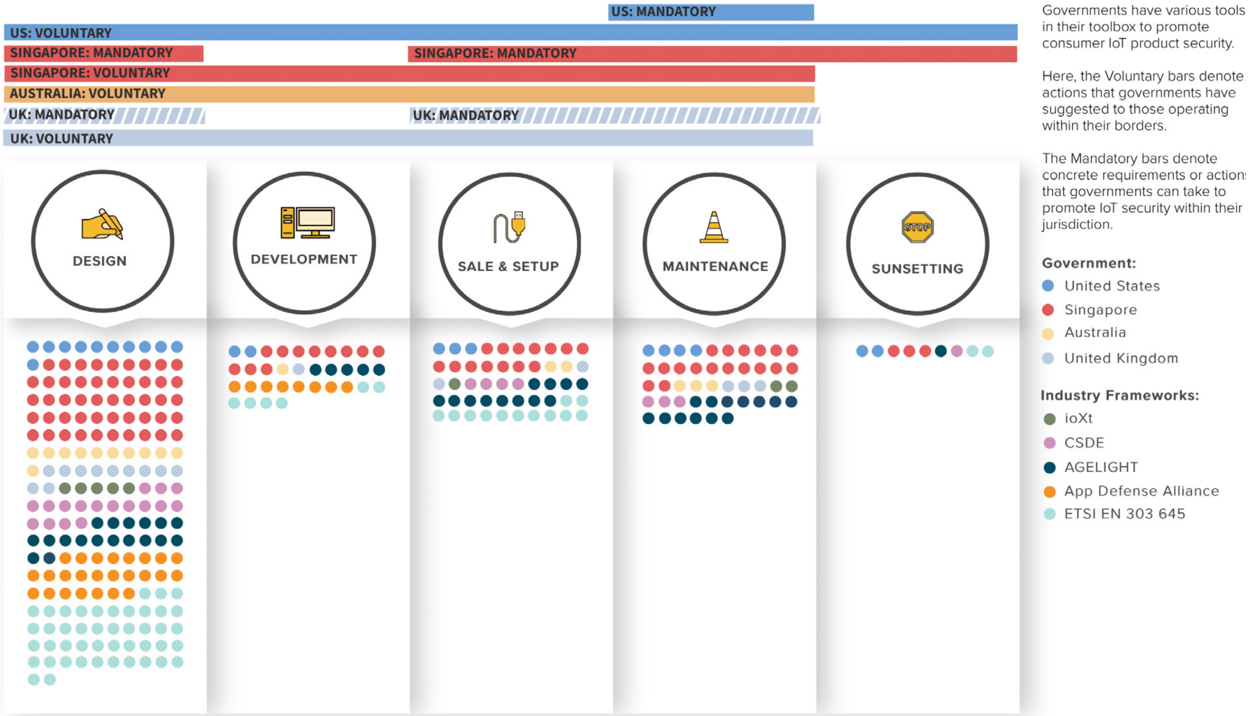
[98] Ron Ross, Michael McEvilley, and Janet Oren, "Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems," National Institute of Standards and Technology, March 21, 2018, https://doi.org/10.6028/NIST.SP.800-160v1.

[99] Department for Digital, Culture, Media & Sport, "The Product Security and Telecommunications Infrastructure (PSTI) Bill – product security factsheet."

[100] Department for Digital, Culture, Media & Sport, "The Product Security and Telecommunications Infrastructure (PSTI) Bill – product security factsheet."

[101] ETSI, "Cyber; Cyber Security for Consumer Internet of Things: Baseline Requirements," European Telecommunications Standards Institute, accessed September 22, 2022, https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf.

Figure 4: Overview of Government and Industry Frameworks



Governments have various tools in their toolbox to promote consumer IoT product security.

Here, the Voluntary bars denote actions that governments have suggested to those operating within their borders.

The Mandatory bars denote concrete requirements or action that governments can take to promote IoT security within their jurisdiction.

SOURCE: Liv Rowley and Justin Sherman for the Atlantic Council.

disclosure policy, and keeping software updated and secure.[102] The provisions around not using default passwords, validating input data, and securely storing credentials are primarily useful in the abstract at the design phase and implemented during the development phase.

The United States, the UK, Australia, and Singapore also have significant guidance and/or requirements at the product *sale and setup* phase. For the ETSI guidance—which underpins guidelines in the UK, Australia, and Singapore—the implementation of a vulnerability disclosure policy comes into play during sale and setup. Singapore's CLS has four levels against which companies can certify products, from baseline requirements, certified based on developer self-declaration, to comprehensive penetration testing conducted by ISO-accredited independent laboratories.[103] And in the United States, the IoT Cybersecurity Improvement Act of 2020 requires NIST to publish "standards and guidance" around IoT product purchasing and shifts the compliance burden from vendors onto federal purchasers.[104] Moreover, federal agencies must consider such factors as secure development, identity management, and patching when looking at buying an IoT product and then prove that said product satisfies NIST's guidance.[105] E.O. 14028 directs federal agencies to implement secure software verification processes and directs NIST, the FTC, and other agencies

[102] "Code of Practice: Securing the Internet of Things for Consumers," the Australian Government, accessed September 22, 2022, https://www.homeaffairs.gov.au/reports-and-pubs/files/code-of-practice.pdf.

[103] CSA Singapore, "Cybersecurity Labelling Scheme (CLS)," Cyber Security Agency Singapore, accessed September 22, 2022, https://www.csa.gov.sg/Programmes/certification-and-labelling-schemes/cybersecurity-labelling-scheme/about-cls

[104] IoT Cybersecurity Improvement Act of 2020, H.R.1668, 116th Cong. (2020). https://www.congress.gov/bill/116th-congress/house-bill/1668.

[105] IoT Cybersecurity Improvement Act of 2020

to identify "IoT cybersecurity criteria for a consumer labeling program."[106]

Regulations enforced by the FTC and FCC likewise focus on IoT product labeling when consumers look to purchase and deploy products (in the FTC's case) and IoT network design (in the FCC's case). This is not to say the US security approach entirely neglects the maintenance and sunsetting phases; NIST's first IoT publication (NISTIR 8259)[107] includes a category for "post-market" security considerations as well as general recommendations for establishing communication channels for product updates and customer feedback. A subsequent update to the document (NISTIR 8259A) contains recommendations for security update features.[108]

All four government approaches focus less on the *maintenance* phase of the IoT product lifecycle. The UK's IoT security approach has gaps in providing manufacturers, vendors, and users with *maintenance* guidance (e.g., once the security update plan is in place and communicated, how will it be continuously followed?) and *sunsetting* guidance (e.g., if the company stops providing security updates, how should they inform users and what options might users have for replacing devices?). While there is some minimal guidance here—for instance, the UK DCMS Code of Practice includes a provision to make the installation and maintenance of products easy—it hardly provides anything substantively useful for manufacturers, vendors, or buyers. The same therefore goes for Australia, which follows the UK's guidance. Singapore does provide detailed guidance on the maintenance phase at Tier 2, 3, and 4 of the certification scheme.

Each approach has significant gaps at the *sunsetting* phase. The United States lacks sunsetting guidance in its IoT security approaches, and regulatory enforcement does not focus on sunsetting (e.g., the FTC focuses on how products are marketed to consumers, not how products are retired). Singapore's labeling scheme program provides little guidance in the way of notifying users about terminated security updates when products are at their "life's end" and then, as a result, posing new and greater security risks. The UK's IoT security approach also lacks sunsetting guidance, such as what happens if a company stops providing security updates as recommended by the DCMS. This means users, and society writ large, may have some protections against IoT insecurity at the earlier phases of the IoT product lifecycle, such as when companies are designing IoT products sold to the government and used in relation to critical infrastructure, or when vendors are advertising their products on the shelf and regulated. Yet, for all the businesses, individuals, and other entities using IoT products that are long past their lifespan, they are exposing themselves to insecurity possibly without even knowing it—and without government policies and security approaches that protect users against the termination of security updates, outdated labels, and other security problems.

It is also important to note that requirements may, in the future, speak to areas outside the device lifecycle as well, concentrating more on an IoT manufacturer's organizational structure or developer training. NIST notes this in their June 2022 NISTIR 8425 initial public draft, titled "Profile of the IoT Core Baseline for Consumer IoT Products."[109] Developer activities, as outlined in NISTIR 8425, may include Documentation, Information & Query Reception, Information Dissemination, and Education & Awareness.[110] Some industry IoT security frameworks include non-device requirements as well. For instance, the IoT Security Foundation's framework mandates the existence of certain roles at a company (for example, 2.4.3.1 mandates "There is a person or role, accountable to the Board, who takes ownership of and is responsible for product, service and business level security, and mandates and monitors the security policy"); or specific actions to be included in a company's security policy (for example, "As part of the Security Policy, provide a dedicated security email address and/or secure online page for Vulnerability Disclosure communications").[111] Such standards that apply to elements outside of the scope of the device lifecycle itself are critical to fostering a stronger security environment overall and should be remembered and considered as IoT security becomes stronger.

[106] The White House Briefing Room, "Executive Order on Improving the Nation's Cybersecurity," The White House, accessed September 22, 2022, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/.

[107] US National Institute of Standards and Technology. *Foundational Cybersecurity Activities for IoT Device Manufacturers*. NISTIR 8259. Michael Fagan et al. Gaithersburg: National Institute of Standards and Technology, May 2020. https://csrc.nist.gov/publications/detail/nistir/8259/final.

[108] U.S. National Institute of Standards and Technology. *Foundational Cybersecurity Activities for IoT Device Manufacturers*. NISTIR 8259A. Michael Fagan et al. Gaithersburg: National Institute of Standards and Technology, May 2020. https://csrc.nist.gov/publications/detail/nistir/8259a/final.

[109] Michael Fagan et al., "Profile of the IoT Core Baseline for Consumer IoT Products," National Institute of Standards and Technology (NIST), June 17, 2022, https://csrc.nist.gov/publications/detail/nistir/8425/draft.

[110] Michael Fagan et al., "Profile of the IoT Core Baseline for Consumer IoT Products."

[111] IoT Security Foundation, "IoT Security Assurance Framework."

4. TOWARD A CONSOLIDATED APPROACH

The framework above underscores how some governments and industry actors are making progress in pushing for greater IoT security—but there is a long road ahead to improving cybersecurity in the IoT ecosystem. There are still some governments and many industry actors underinvesting in IoT security. Despite their stated concerns, consumers continue to purchase insecure products. As a result, product manufacturers and vendors need to deliver meaningful transparency and improvements in user security outcomes. Without the predictability of common security standards that impose pressure on all manufacturers and vendors, proactive firms have little incentive to produce secure products, and there are few penalties for laggards.

Overcoming Widespread Risks

Promisingly, the past few years have seen a flurry of activity on IoT security from governments, industry groups, and consumer advocates. The attitude among those interviewed for this report generally was optimism about the direction of travel, with concern over the pace of the trip. Singapore is nearly two years into a voluntary, four-level labeling scheme that will be gradually expanded as mandatory by product type, as it currently is for internet routers. Australia appears poised to pursue a labeling approach that mirrors Singapore's four levels ("graded shield") or a simpler indicator showing the timeframe that security updates will be provided ("icon expiry"). The UK has rejected the concept of labels and is instead on the cusp of passing legislation that empowers regulators to set basic cybersecurity requirements for all smart devices, a baseline that can be ratcheted up over time. In the United States, two states have implemented their own minimum security requirements, federal agencies must purchase products with more robust security, and NIST recently recommended a binary label akin to approaches in Germany and Finland. Consensus standards, enforcement measures, and international cooperation across these four jurisdictions are feasible but not yet close. Nevertheless, there still are threats to progress:

- **Risk #1: Regulations, standards, and norms diverge between jurisdictions.** Despite today's promising signs, as more jurisdictions take on the problem of IoT insecurity, there is a risk that regulatory divergence worsens with an 'every-market-for-themselves' approach where duplicative requirements and confusing enforcement schemes burden IoT vendors who must work to support multiple sets of standards or elect to focus on a small set of jurisdictions.

- **Risk #2: Cybersecurity labels fail to demonstrate value to both manufacturers and consumers.** One interviewee summed up the attitude toward cybersecurity labels with an analogy to Churchill's famous quote about democracy: "the worst option, except for all the others." Labels are an increasingly popular approach in national IoT security efforts. Despite a clearly articulated demand for greater security by consumers, some observers are doubtful that consumers can or will make informed cybersecurity decisions even with the benefit of an indicator on the box or the webpage. Others question whether it is correct to task consumers with making such security decisions for themselves, comparing insecure IoT products to an unsafe lightbulb: you do not compare lightbulb brands to see which one is least likely to explode. Like other market signals, cybersecurity labels can suffer from a collective action problem, only arising if both sides of a transaction value them.

- **Risk #3: Product security requirements become watered down as they approach broader adoption.** Particularly in the United States, legislation often becomes less potent as it approaches the federal level. Industry resistance was sufficient to kill prior versions of the IoT Cybersecurity Improvement Act and cut some of the provisions that were finally passed in its 2020 version.[112] Given federal law's preemptive power, consumer IoT security legislation could counteract more ambitious measures at the state level. This dynamic may also occur internationally if jurisdictions are driven to the lowest common denominator in pursuit of consensus.

[112] Robert Lemos, "New IoT Security Bill: Third Time's the Charm?" *Dark Reading*, March 2019. https://www.darkreading.com/iot/new-iot-security-bill-third-time-s-the-charm-.

- **Risk #4: Guidelines become too rigid, locking in outdated security practices.** As Brian Russell and Drew van Duren describe, "The greatest challenge in the security industry is finding methods today of defending against tomorrow's attacks given that many products and systems are expected to operate years or decades into the future."[113] Legislation must define processes and outcomes rather than codifying specific security measures that might soon become irrelevant.

- **Risk #5: The drive for improved consumer IoT security fails to have an impact on product manufacturers in jurisdictions without strong IoT security laws.** The national initiatives surveyed in this report focus primarily on efforts to effect change by imposing requirements on products sold in each one's jurisdiction, as opposed to trying to impact what happens where products tend to be manufactured, citing the challenge of extraterritorial enforcement. Interventions must consider the full range of actors who can put pressure further up the supply chain, with retailers, in particular, having the potential to play an influential role.

The Shape of a Consolidated Approach

What might a better IoT future look like? One description is: "a world in which every IoT ecosystem stakeholder['s] choices and actions contribute to overall security of IoT where consumers and benefactors are simply secured by default."[114] It could be raising the tolerable level of insecurity to the point where consumers trust IoT products and services as something more than a roll of the dice.

Crucially, this world must reflect different economic incentives for manufacturers, consumers, and attackers. Policy change is necessary to help shape and channel these incentives. When assessing any proposal, one should consider its ability to advance the following outcomes:

- Eliminate the most glaring insecurities in consumer IoT products, thus increasing the level of effort and sophistication required for attackers to compromise them.

- Promote harmonization across jurisdictions, avoiding needless divergence and duplication, thereby reducing friction for manufacturer uptake.

- Sharpen incentives for manufacturers to exceed the minimum baseline of security practices.

- Increase consumer awareness of the risks from insecure products and increase interest in security as a feasible and accessible buying criterion.

- Provide real impact on user security outcomes in the near term while maintaining flexibility to incorporate new controls through consensus measures as technology evolves.

To drive the above outcomes and closer alignment in policy across these four states, the team proposes a multi-tiered IoT product labeling and certification scheme with basic, easily understandable labels for consumers (Figure 5). This multi-tiered scheme would ensure that minimum security standards are met, give consumers easily digestible ways of understanding the security of a product, and allow manufacturers that invest in higher security to advertise it understandably.

[113] Brian Russell and Drew van Duren. *Practical Internet of Things Security – Second Edition*, Packt Publishing, (Birmingham, UK: 2018).

[114] Eustace Asanghanwa, "Solving IoT device security at scale through standards," Microsoft (blog), September 21, 2020, https://techcommunity.microsoft.com/t5/internet-of-things-blog/solving-iot-device-security-at-scale-through-standards/ba-p/1686066.

Figure 5: Overview of IoT Security Tiers

	Definition	Scope	Example Device Capabilities	Example Certification / Enforcement Schemes
Special Standards for Safety Critical Devices	Vertical-specific rules for devices that could directly threaten lives if compromised.	Medical devices Motor Vehicles	Process for assessing the severity of patient harm if a vulnerability is exploited Measures that allow rapid recovery from incidents	FDA Medical Device Certification Federal Motor Vehicle Safety Standards
Tier 2: Enhanced Security Features	Desired cybersecurity features that manufacturers should be encouraged to adopt but may not be suitable in all scenarios/product types. Certifiers can further subdivide this tier as fits the interests of vendors and consumers. Over time, it is anticipated that many of these features will migrate to Tier 1.	Smart home devices Networking devices and telecom gear	Sensitive security parameters in persistent storage stored securely Device uses best practice cryptography to communicate securely Device has no known software vulnerabilities Consumers provided with info on telemetry data collected/ processed Personal data is secured / can be deleted by user Vendor uses secure development practices	Singapore CLS – Level 3 & 4 Finland Cybersecurity Label Germany BSI IT Security Label (Note: Relative positioning of examples does not represent a security hierarchy among these programs)
Tier 1: Minimum Baseline Features	High-value measures that should be mandatory for all consumer IoT devices.	Smart home devices Networking devices and telecom gear	Keep software updated Vulnerability disclosure contact No universal default passwords	Singapore CLS – Level 1 / UK PSTI Law ("Top 3" Baseline) California SB-327 /Oregon HB 2395

SOURCE: Patrick Mitchell for the Atlantic Council.

Tier 1: Minimum Baseline Features. The first tier should be a set of mandatory, baseline, self-attested IoT security standards created by governments in consultation with industry. For each country, the government agency leading this effort should ideally be the organization already in charge of cybersecurity standards, and if there is not one, governments should select an organization with a high degree of transparency, technical competence and capacity, and a track record of working with industry and civil society. The recommended baseline security standards should be rooted in widely agreed upon desirable security outcomes, for instance, the core principles outlined in ETSI EN 303 645—such as eliminating default passwords, mandating a vulnerability reporting contact, and facilitating secure updates for software. Once governments set this tier, manufacturers should apply with the agency administering the program and self-attest that they meet these standards. The agency should then provide qualifying products with a label indicating that they have met these baseline requirements, and the manufacturer and product vendor (if different than the manufacturer) should include this label and information about it in the product description. Random audits can assess compliance without the need for a time-consuming and expensive certification process. Examples of national programs in this tier include the UK's PSTI Bill, Singapore's CLS Tier 1 requirement for routers, and California and Oregon's IoT security laws.

Tier 2: Enhanced Security Features. Building off the first tier of mandatory, baseline, self-attested IoT security standards, governments should then work with industry to set a second tier of security standards—higher, voluntary, and independently tested. The standards to qualify for this second tier should likewise look to the Tier 1 baseline as a starting point, with a particular focus on ensuring products communicate securely and protect consumers' personal data, inspired by security outcomes that may be drawn from ETSI EN 303 645. Qualifying products will receive a label indicating that they have both met the Tier 1 baseline requirements and the Tier 2 requirements, and the product description should include information about this label. To encourage the uptake of the second tier, securing a label should be a relatively cheap and quick process. Given that some jurisdictions may see more value in a scheme with more than two tiers, national regulators should be able to subdivide this tier into different levels of security. Examples of existing programs that would fall within this tier include Levels 3 and 4 of Singapore's CLS, Finland's Cybersecurity Label, Germany's BSI IT Security Label, and the binary label recommended by NIST in the United States.

Special Standards for Safety Critical Products. Industry-specific regulators should remain in charge of setting the highest bar of security standards for IoT products that present an imminent threat to human life if compromised. For most smart devices, consumers do not bear the brunt of the consequences if their device is vulnerable to an attacker. This dynamic shifts dramatically when the connected device is an automobile or pacemaker and the consequences become potentially lethal. In these instances, however, consumers still lack the expertise to assess risk. These industries tend to already have specific regulators focused on product safety: for example, the FDA certifies medical devices, and the National Highway Traffic Safety Administration (NHTSA) is charged with enforcing motor vehicle safety standards. In this context, an internet connection is merely another feature that introduces new risks to product safety. These regulators should look to standards bodies such as ETSI and NIST as a starting point for guidance on cybersecurity, but the ultimate requirements for these safety-critical applications must extend to the particular security needs of the industry—which are likely even more stringent than the second tier discussed above. Products that fall into this category need not be certified with a label. Instead, if they fail to meet the regulator's minimum standards, they should not be approved (or should be recalled if they are already on the market).

What Does the Label Look Like?

A label for IoT security should consist of a standardized table or graphical description of security features, attached physically to a product box and digitally affixed to product descriptions online. The digital description of an IoT product's security features is especially important, and—given the constantly changing security landscape—keeping digital labels up-to-date is often easier than doing so for physical labels. Ideally, the standardized-format description of product security features should be mapped to a set of standard IoT security criteria—such as a checklist of product compliance with some NIST security best practices, or a checklist of product compliance with ETSI requirements for IoT security (e.g., does this product use universal default passwords, does it have a security update function in place). Labels, intended for audiences ranging from consumers to enterprise purchasers, should use clear, easily understandable language to describe product security features, rather than referencing specific standards numbers or using highly technical verbiage (such as describing a specific encryption algorithm).

Related to the label, governments should consider cooperating and coordinating with industry to ensure data on labels is easily accessible—to regulators, researchers, and the public generally. One idea is creating a central repository of manufacturer and vendor label information, perhaps maintained by a country's cybersecurity standards organization or a standards development organization (SDO), into which vendors and manufacturers can upload independently tested and/or self-certified label information about IoT product security. It may be advantageous to develop a single form containing information of interest to multiple major jurisdictions, inspired by the "Common App" form which allows individuals to fill out one form to apply to multiple US-based universities. This would allow regulators and others to access information on company compliance and broader IoT product security trends in a single place and in a single, accessible format; it also potentially streamlines compliance efforts by IoT vendors, allowing them to file security information about their products in one place that is applicable in multiple jurisdictions. Another idea is having companies make this information available from their systems through a standard API—such that all the information is not stored in one single place, and the government does not have to maintain a central repository of IoT security label data, but that individuals can query manufacturer and vendor APIs to get label information.

A Note on Ambitions

At their simplest, today's approaches reflect two different philosophies about where governments should focus their efforts: (1) targeting the "low hanging fruit" of higher impact/lower effort measures with mandatory requirements, or (2) setting an optional higher bar and trying to get consumers and industry to care about it. The former arguably views security improvements as a rising tide that fills in the lowest lying areas first, while the latter arguably views it as a distant target that focuses our gaze, even if not everything hits the bullseye. While both strategies have their merits, they need not be mutually exclusive. We cannot content ourselves with merely getting rid of the worst shortcomings. Similarly, the choice for consumers should not be between one class of products that have poor security and another with world-class security.

It would be counterproductive to suggest that these countries should scrap their national approaches in favor of a new consensus program. Given how recent these efforts are—if they have even yet been implemented—it is still too soon to tell how each country's approach will fare. A degree of national-level experimentation can help determine what does and does not work. Further, as one interviewee noted, while standards may harmonize internationally, enforcement occurs locally. Many jurisdictions have lined up behind the same set of guidelines in ETSI EN 303 645, with some others pursuing slightly differing approaches that nonetheless seek the same outcomes that the ETSI documentation aims to achieve. But the measures chosen to encourage (or compel) industry to generate products with better security must reflect the jurisdiction's regulatory and consumer cultures. The silver bullet is not necessarily a new global label, new methods of enforcement, or new standards for IoT products. Instead, the world needs a better way of bringing together these efforts and ensuring they continue to avoid contradiction and duplication.

5. RECOMMENDATIONS

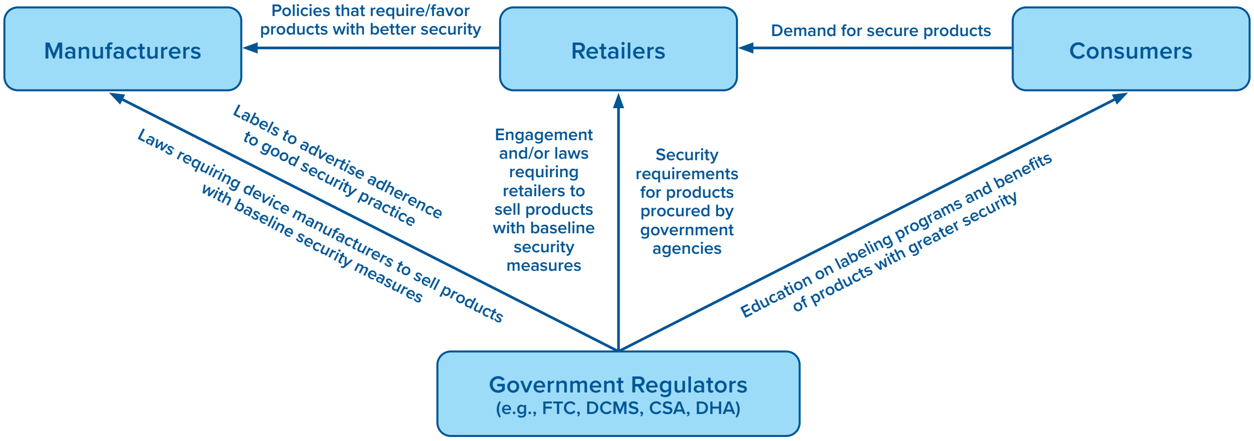
This section lays out nine recommendations for government and industry actors to enhance IoT security, broken into three recommendation sets: setting the baseline of minimally acceptable security, incentivizing above the baseline, and pursuing international alignment on standards and implementation across the entire IoT product lifecycle. While many of these recommendations apply generally to those interested in promoting a more secure IoT ecosystem, the report also aims to identify specific actors and the steps they can take to bring about this multi-tier structure for IoT security (Figure 6). Moreover, these recommendations also aim to address the risks and uncertainties described in the prior section.

Importantly, this report deliberately does not prescribe a particular label design, such as a table or graph. Moreover, it does not prescribe "how" companies should pair physical and digital labels nor to "what" extent companies and/or governments should harmonize specific label designs and digital characteristics across jurisdictions. These areas deserve more work, and the optimal approaches remain unclear at this stage.

Recommendation Set: Establish the Baseline of Minimally Acceptable Security (Tier 1): Currently, many governments lack baseline security standards for IoT products, and for some of those that do have such standards enacted, companies must go through a time- and cost-intensive process of independent testing and certification. This substantially raises the barrier to adopting what should be easily achievable and cybersecurity-bolstering baseline standards. By setting this minimum baseline, making it low-cost for companies to comply with, selecting criteria that greatly increase cybersecurity (like no universal default passwords[115] and having security updates), and making it mandatory, governments can ensure IoT products within a country have the most basic and critical security measures in place. In some jurisdictions, enforcement might look like a law that requires every IoT manufacturer to implement the government-set IoT security baseline standards; in other countries, enforcement might look like a consumer regulatory agency creating a new rule within its existing authorities.

IoT products are currently so insecure that hacking them is relatively trivial. The insecurities these products have are so glaring and egregious that even relatively unskilled hackers can get into the game and claim their slice of the pie. Implementing mandatory minimum security standards would have an impact on the state of IoT security by plugging those widely known and easy-to-find holes, which raises the cost of knowledge, time, and resources required to compromise IoT products. In other words, this would help push small fry hackers out of the scene, and the more sophisticated hackers would have to invest energy into developing ways to target more secure products.

Figure 6: Overview of Actors and Actions to Improve IoT Security


Manufacturers
Policies that require/favor products with better security
Retailers
Demand for secure products
Consumers
Labels to advertise adherence to good security practice
Laws requiring device manufacturers to sell products with baseline security measures
Engagement and/or laws requiring retailers to sell products with baseline security measures
Security requirements for products procured by government agencies
Education on labeling programs and benefits of products with greater security
Government Regulators (e.g., FTC, DCMS, CSA, DHA)

SOURCE: Patrick Mitchell for the Atlantic Council.

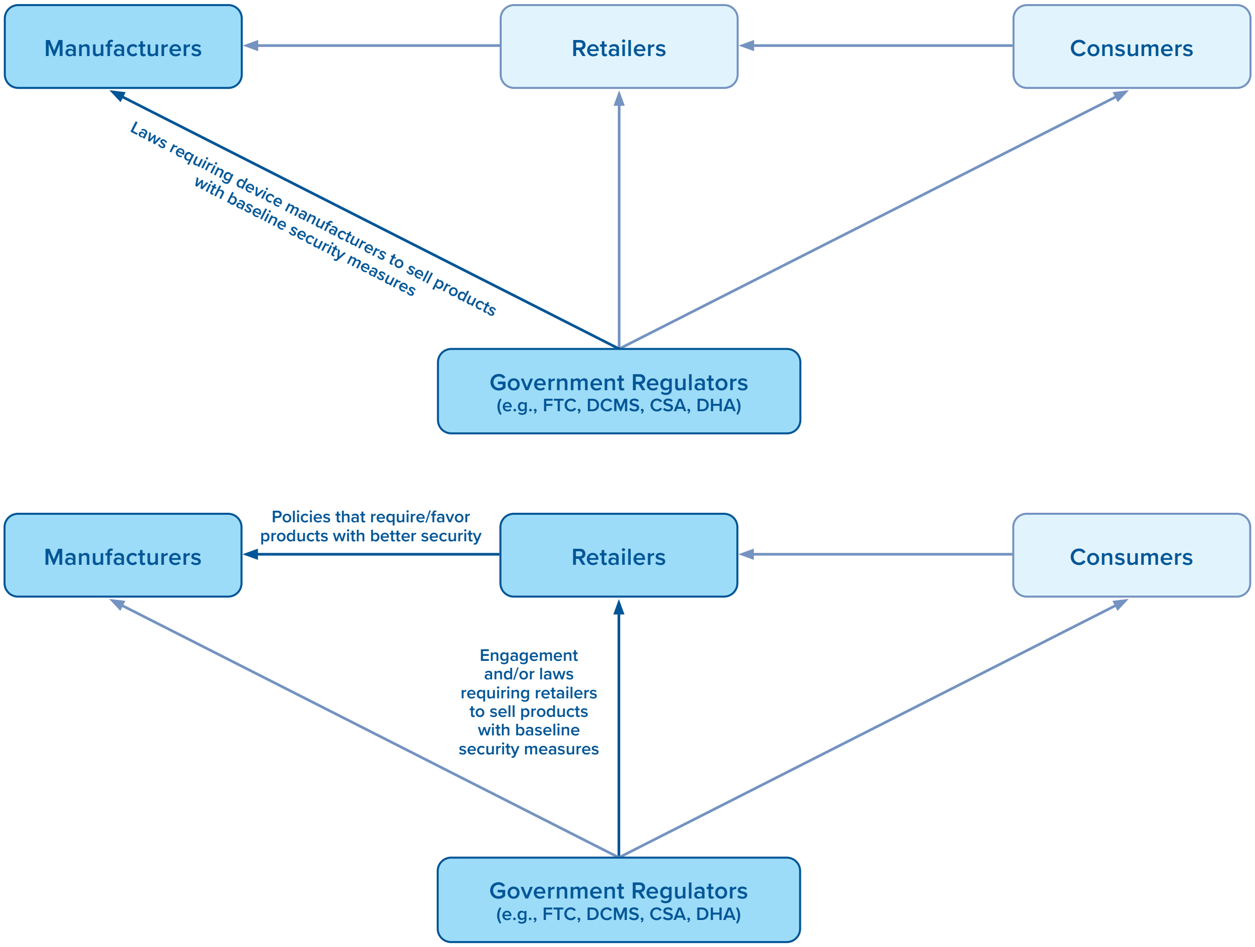
[115] To the reader, this is not to say that organizations should always use passwords as the go-to authentication mechanism in the future—but that if organizations are doing so now, they should not use universal default ones.

To illustrate this point, the Global Cyber Alliance's October 2021 report "IoT Policy and Attack Report" provides a glimpse into just how effective some of these minimum security measures can be.[116] Using a "honeyfarm" (a large network of IoT device honeypots), the Global Cyber Alliance was able to measure the number of attacks against different classes of IoT products and determine whether the number of successful attacks against the target changed, given the implementation of different security standards. For instance, the report found that of over 7,000 malicious login attempts, attackers were only able to login and thereby compromise a device in 79 instances. Those 79 instances all involved devices that used default passwords

This section describes two recommendations that aim to influence two critical groups of actors in implementing this baseline: product manufacturers and retailers.

- **1: Governments should implement regulatory measures to enforce a mandatory baseline on manufacturers selling in their markets (Figure 7).** Initially, governments should conduct outreach to encourage compliance and spread awareness among manufacturers about the security requirements. Inevitably, some companies will not implement the Tier 1 security baseline within the required window or in the required way. This could be the result of many factors, including a lack of awareness about the

Figure 7: Setting the Baseline of Minimally Acceptable Security (Recommendation 1)


Manufacturers
Retailers
Consumers
Laws requiring device manufacturers to sell products with baseline security measures
Government Regulators (e.g., FTC, DCMS, CSA, DHA)
Manufacturers
Policies that require/favor products with better security
Retailers
Consumers
Engagement and/or laws requiring retailers to sell products with baseline security measures
Government Regulators (e.g., FTC, DCMS, CSA, DHA)

SOURCE: Patrick Mitchell for Atlantic Council

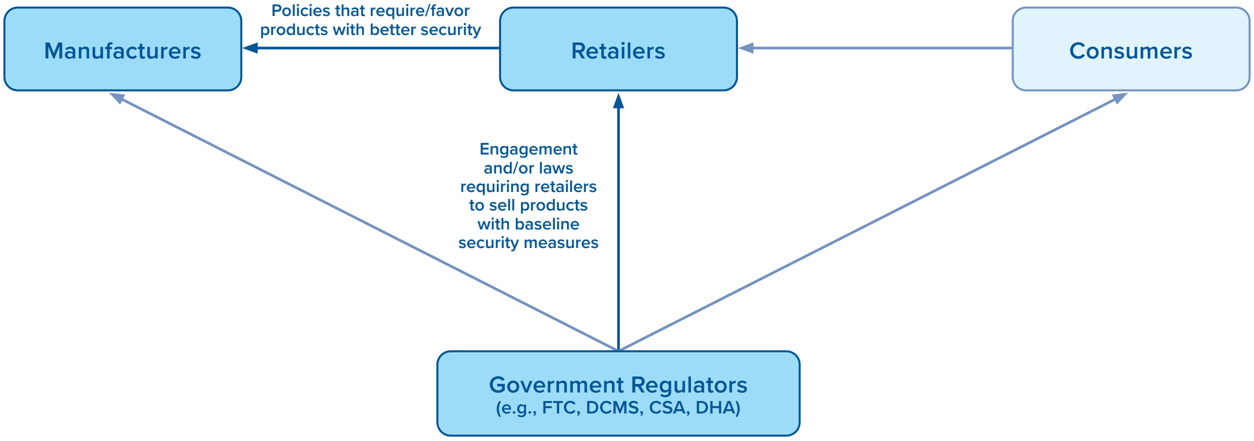
[116] *GCA Internet Integrity Papers: IoT Policy and Attack Report*, Global Cyber Alliance (GCA), October 2021, https://www.globalcyberalliance.org/wp-content/uploads/IoT-Policy-and-Attack-Report_FINAL.pdf.

rule (e.g., for smaller IoT manufacturers), feet-dragging, and limited capacity to quickly implement the self-attested label and certification, among others. Governments should therefore develop mechanisms to publicize the new, required security baseline at Tier 1 and encourage companies to implement it within the specified window. Beyond general public education campaigns, for example, this could include such processes as a country's key standards agency holding sessions with industry to explain new requirements and answer any questions that may arise—well before the requirements go into effect.

Next, governments should set up random audit mechanisms to ensure firms' claims are accurate and issue penalties as needed. Some companies may self-attest to a security baseline and then take action that deviates from that attestation (e.g., implementing security updates and then ceasing security updates). Other companies may falsely self-attest to the security baseline altogether. If a product has been falsely attested to and does not meet the minimum security standards, the government should begin by issuing a compliance notice to its manufacturer. The compliance notice (or prompt for change) should outline all corrective actions and set a clear deadline for when these actions must be complete. Should a manufacturer continue to produce a noncompliant product with a falsely advertised security label, the government's relevant enforcement agency should issue a stop notice that orders the manufacturer to cease selling the product until made compliant. The agency's stop notice (sent to the company and published publicly) should also demand the recall of the noncompliant product. The agency should also consider additional actions depending on its authorities and typical enforcement processes against other companies domestically, such as fines. In line with other contexts in which companies may hold liability, governments carrying out enforcement should weigh whether a reasonable effort was made to attest in good faith, among other factors.

- **Recommendation 2: Governments should follow the "reversing the cascade" philosophy, where instead of trying to influence manufacturers based abroad, governments put pressure on domestic suppliers and retailers—who may, in turn, put their own pressure on manufacturers to improve security (Figure 8).** It is not just governments that make policy decisions that impact product manufacturers. There is considerable power in the terms and conditions for selling through major marketplaces and retailers like Amazon, Walmart, and Target. Many IoT security efforts encounter issues when they try to levy penalties on manufacturers, as many of them are based outside their jurisdiction and may not have incentives to comply with security requirements. Vendors, however, fall within a government's jurisdiction, making actions more feasible. There are also fewer major IoT vendors than there are IoT product manufacturers, allowing efforts to be more concentrated. In the US, political leaders and regulatory agencies, such as cybersecurity officials in the Department of Commerce and regulators at the FTC, should call upon major retailers to more proactively police the sale of consumer IoT products that lack basic security features. This is because these retailers currently sell products like smart thermostats, smart speakers, and

Figure 8: Setting the Baseline of Minimally Acceptable Security (Recommendation 2)


Manufacturers
Policies that require/favor products with better security
Retailers
Consumers
Engagement and/or laws requiring retailers to sell products with baseline security measures
Government Regulators
(e.g., FTC, DCMS, CSA, DHA)

SOURCE: Patrick Mitchell for Atlantic Council baby monitors that have poor security practices and use default passwords. If engagement does not bring about change, retailers could be held accountable through new laws that penalize them for the sale of noncompliant products. Though, targeting noncompliant smart products that have been sitting for a long time on the shelf may achieve higher security across products more quickly, without creating barriers to entry for small manufacturers. It is also possible that the FTC could pursue action against specific retailers under its "unfair or deceptive acts or practices.[117]

As the world's largest online retailer, Amazon, for example, could have an outsized impact with an expansion of its "Restricted Products Policy" to bar unsafe smart devices. When contacted by security researchers about a particularly vulnerable wireless camera (promoted as "Amazon's Choice") the firm removed the preferred listing and responded, "We require all products offered in our store to comply with applicable laws and regulations and have developed industry-leading tools to prevent unsafe or non-compliant products from being listed in our stores."[118] In this vein, in its Examples of Prohibited Listings in the Electronics category, Amazon should explicitly prohibit smart home products that fail to meet the Tier 1 requirements. The US government has the ability to apply pressure on online retailers (not just Amazon) to do that, such as through public messaging campaigns and convenings with company executives through organizations like NIST. If this fails to stem the presence of insecure products on the site, another measure could include requiring firms to receive approval before listing consumer IoT products—as they must for categories including jewelry, DVDs, and "Made in Italy" items—or just a subset of high priority items like children's connected toys. This approval could be as simple as submitting a form that attests that the firm does not use universal default passwords and lists a vulnerability reporting point of contact. Amazon's application form for selling streaming media players could serve as a template. Even without specific laws that force its hand, this policy would be in line with Amazon's stated goal of allowing customers to buy with confidence on its platform.

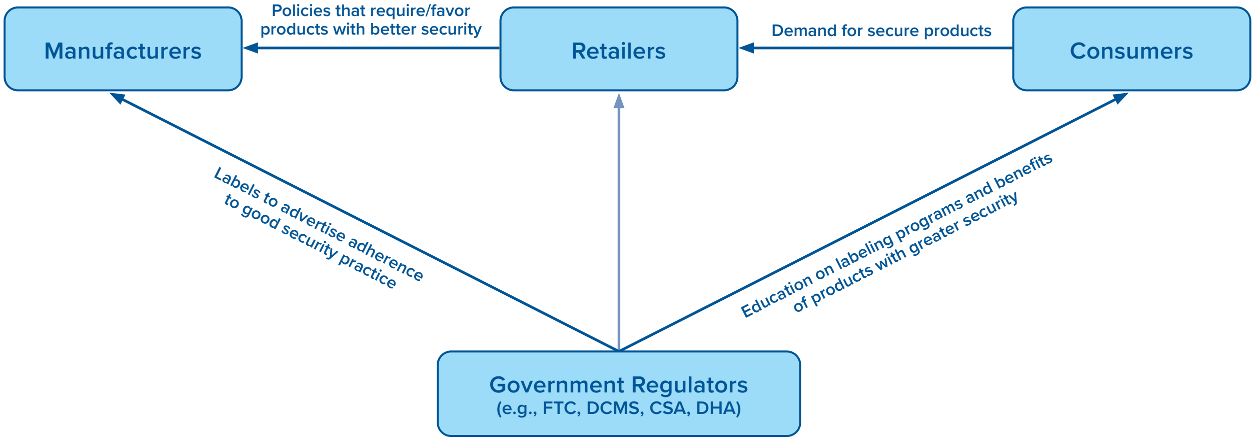
Recommendation Set: Incentivize Above the Baseline (Tier 2): Ensuring that all smart devices meet basic security requirements is valuable, but insufficient relative to the present risk in the IoT ecosystem. Some buyers may wish to achieve security at a higher level, and even more likely, some governments may wish to require manufacturers to adopt security standards above the first-tier baseline. Some manufacturers may also pursue a higher level of security as a differentiator. This section outlines four recommendations that will strengthen the development of this higher tier: setting the higher tier, mandating a more stringent degree of security for government-procured smart devices, expanding label recognition between states, and moving towards a consensus certification and labeling program. These actions will grow demand for secure products, increase consumer awareness, and decrease friction for firms that must otherwise navigate multiple certification regimes.

- **Recommendation 3: Governments should support the creation of a voluntary, higher tier of security requirements, indicated via labeling programs in their markets (Figure 9).** The objective of this tier is to encourage firms to adopt more advanced security features and design practices in their products. As with the first tier, the specific security provisions that governments select for this tier should consider outcomes-based approaches, perhaps looking to ETSI EN 303 645 for inspiration. Other provisions, such as those from OWASP and ioXt, can supplement such approaches. Unlike the first tier in which companies self-attest to meeting standards, in this tier, companies should have their products evaluated and their status certified by a third-party testing lab. These approved labs should be certified under ISO/IEC 17025, an internationally accepted standard for Testing and Calibration Laboratories, to ensure consistent application of device security testing procedures. Since product certification at this tier is on a voluntary basis, manufacturers will likely wish to advertise their products' enhanced security features. Any device that passes the test and therefore shown to meet the Tier 2 requirements will receive an accompanying Tier 2 label. These labeling schemes can be "binary," indicating the presence or lack of desired security features (e.g., Finland and Germany's programs), or multi-level, allowing manufacturers to pursue the certification that meets the desired "grade" of security for their product (e.g., Singapore's CLS). After issuance, random audits should ensure that devices continue to remain in compliance with the provisions of their label. If a product has received a label but no longer meets its requirements, the government should decertify the product. Depending on the jurisdiction, the government may also pursue legal action against those who willfully make false claims about their product's security features.

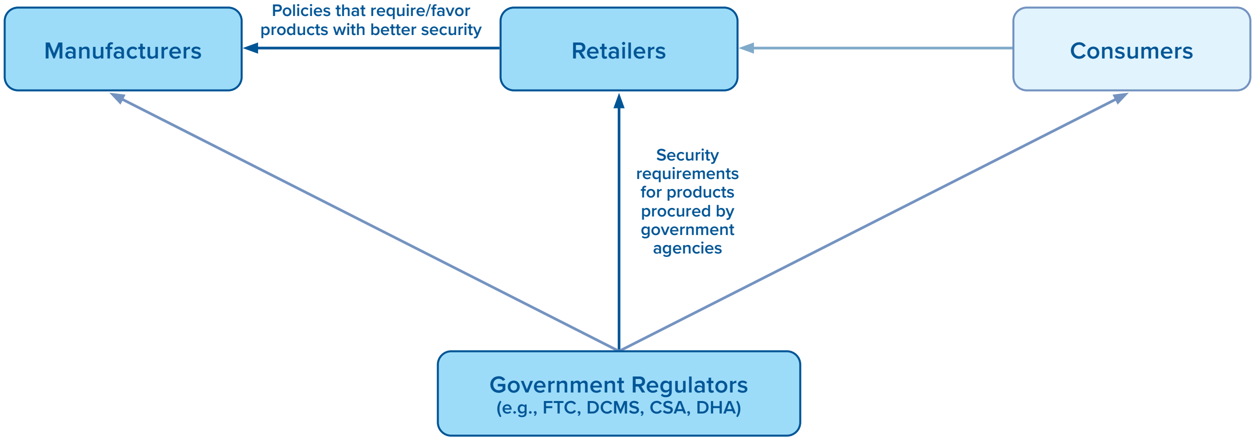
[117] 15 U.S.C. § 45, "Unfair Methods of Competition Unlawful; Prevention by Commission," https://uscode.house.gov/view.xhtml?req=(title:15%20section:45%20edition:prelim)%20OR%20(granuleid:USC-prelim-title15-section45)&f=treesort&edition=prelim&num=0&jumpTo=true.

[118] Andrew Laughlin, *How a smart home could be at risk from hackers*, Which? 2021, https://www.which.co.uk/news/article/how-the-smart-home-could-be-at-risk-from-hackers-akeR18s9eBHU.

Figure 9: Incentivizing Above the Baseline (Recommendation 3)


Manufacturers
Policies that require/favor products with better security
Retailers
Demand for secure products
Consumers
Labels to advertise adherence to good security practice
Education on labeling programs and benefits of products with greater security
Government Regulators (e.g., FTC, DCMS, CSA, DHA)

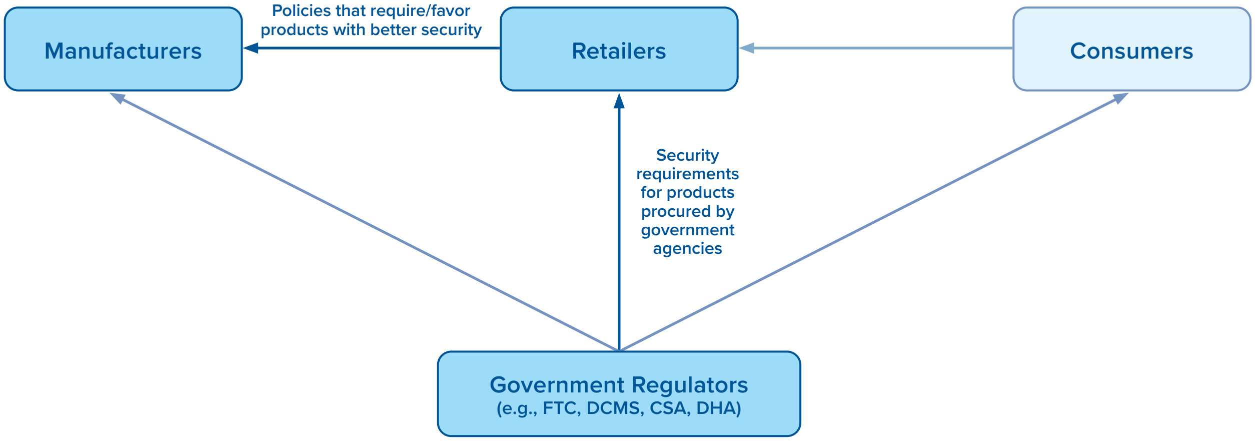
SOURCE: Patrick Mitchell for the Atlantic Council.


Manufacturers
Policies that require/favor products with better security
Retailers
Consumers
Security requirements for products procured by government agencies
Government Regulators (e.g., FTC, DCMS, CSA, DHA)

SOURCE: Patrick Mitchell for the Atlantic Council.

The existence of the second tier will aid in raising the security of IoT products above the minimum standards set in tier one. As the multi-tier model evolves over time, governments can also migrate effective standards from the second tier over to the first tier. Further, using outcomes-based approaches such as ETSI EN 303 645 as inspiration for these security requirements will ensure continued momentum around many agreed-upon basic security principles, while the employment of public-private cooperation ensures that standards are actionable. To drive the uptake of labeling programs, governments should engage with industry and the public to spread awareness of the programs' benefits, and they may also consider defraying start-up costs, such as waiving registration fees and subsidizing testing expenses. Much like ETSI could serve as a guiding foundation for establishing a set of baseline security requirements for Tier 1, the industry security efforts underway by the CTA and the CSA, among others, could become a foundation for establishing a higher bar of IoT product security paired with a consumer-facing IoT labeling scheme.

Figure 10: Incentivizing Above the Baseline (Recommendation 4)


Manufacturers
Policies that require/favor products with better security
Retailers
Consumers
Security requirements for products procured by government agencies
Government Regulators
(e.g., FTC, DCMS, CSA, DHA)

SOURCE: Patrick Mitchell for the Atlantic Council.

- **Recommendation 4: Governments should include Tier 2 requirements as part of government procurement contracts (Figure 10).** Technology manufacturers and vendors strongly benefit from government contracts, and the inclusion of cybersecurity standards in government procurement requirements can be one mechanism to incentivize large and small manufacturers to adopt them. The cost-benefit is simple for those companies: if they do not meet the specified cybersecurity requirements, they do not qualify for government contracts. Governments should therefore include Tier 2 (or higher) security standards in their procurement requirements such that any IoT manufacturer or vendor who wishes to do business with them must invest in a higher level of security beyond the Tier 1 baseline.

  The United States provides a recent case study in this approach with its IoT Cybersecurity Improvement Act of 2020, which requires federal agencies to abide by NIST cybersecurity guidelines when procuring IoT products. Thus, companies will not be able to sell their IoT products and services to the US federal government without complying with NIST cybersecurity guidelines. Procurement requirements in the UK, Singapore, and Australia, especially in the defense apparatuses, can similarly provide a mechanism by which the government can incentivize the adoption of a higher tier of cybersecurity practices. Since it tends to be too unwieldy for companies to produce multiple lines of the same product—one suitable for the government's requirements and a separate less secure model—the entire market would benefit. This measure would not only incentivize companies to act but would also mean that IoT products used by governments will themselves have a higher bar of security. In turn, procurement is a mechanism by which to better protect government systems and, likely, citizen data against cyber risks as well.

- **Recommendation 5: In the short term, governments should reach agreements to mutually recognize each other's labels.** As different national IoT labeling schemes proliferate around the world, it will be important to reduce the burden on manufacturers from duplicative testing and certification requirements. In October 2021, Singapore and Finland agreed to mutually recognize each other's labels for IoT products, hoping that this agreement will also spur more international collaboration. Through this agreement, companies that receive Finland's Cybersecurity Label for a product are immediately eligible for Singapore's Level 3 label, and vice versa. Even though not a country focused on in this report, Germany's voluntary cybersecurity labeling program went live in January 2022, and it is reportedly in discussions with other countries to further expand mutual recognition. Given ETSI EN 303 645's role as the backbone of multiple national frameworks, these agreements would likely be relatively simple to establish, recognizing that some agreements might focus on recognizing specific requirements while others might focus on recognizing equivalency—when similar outcomes are achieved with slightly different requirements. Major technology firms that care about improving the security of smart devices can apply for certification, even if it does not immediately benefit them, thus adding to the credibility of labeling programs. Countries with labeling programs already underway should study their impact, consider stakeholder feedback, adjust their schemes as needed, and share lessons learned with other countries interested in adopting this approach. It would be helpful for some of the analysis to focus on how to balance the need for maintaining high standards with reducing the administrative burden on firms going through the certification process. Major IoT vendors have noted how onerous it is to submit their products to multiple IoT security certification processes; for smaller firms, it can only be more difficult. Solutions like a "Common Application form"—inspired by the innovation that allows individuals to apply to multiple US-based universities by filling out one document—could help address this problem, as can regularly reviewing program-specific requirements and dropping ones that do not add value.

- **Recommendation 6: Over the longer term, governments should compare results of their national labeling programs and move towards a single global model for communicating security characteristics of an IoT product.** As regulators in each of the four countries gather performance data on the impact of their approaches, they should work to adopt the attributes of the certification scheme(s) that show the most promise. Labels are already moving well past static data forms with the inclusion of commonly accepted machine-readable formats and more dynamic data sources like SBOMs might be contemplated. Most fundamentally, any future consensus model to communicate the security characteristics of an IoT product (not its packaging) should include basic, easily understandable information affixed to the product, as well as more detailed and dynamic information found online.

  Oftentimes, companies' currently issued IoT security labels and certifications fail to articulate exactly what certification means and how users should understand security. Further, by the time many consumers read an IoT product label, it is already unboxed and undergoing set-up in their home. These shortcomings impede buyers' ability to understand IoT product labels and certifications—thus undermining their effectiveness. As part of this multi-tier framework, government and industry should ensure that at their respective tiers, labels issued for IoT products have basic, easily understandable information affixed to the product itself. They should also ensure the same information is available online, supplemented with other details that manufacturers and vendors can more easily update over time. Instead of communicating in the highly technical language used by experts, governments and industry should look to their relevant communicators for help employing the clearest language possible: for instance, saying, for Tier 1, "No default passwords" on a box and then include a check mark next to it. Doing so will empower buyers to easily make decisions about the security and privacy of a product through easy-to-understand labels.

Recommendation Set: Pursue international alignment on standards and implementation that cover entire IoT product lifecycle: Coherence between jurisdictions on enforcement mechanisms is important, but consistency in the principles of good security practice that form their foundation is even more critical. Given that security is a moving target, regulators must also be able to adapt as capabilities and threats shift. This section describes three recommendations that are key to these objectives: maintaining consensus on standards and scope, introducing regular reviews to keep IoT security programs up-to-date with technological change, and ensuring that all phases of the IoT lifecycle are appropriately addressed.

- **Recommendation 7: Governments should pursue outcomes-based approaches to consumer IoT security rooted in agreed-upon basic security principles and maintain similar definitions for products considered "in-scope."** Efforts to secure consumer IoT should be rooted in widely recognized desirable security outcomes, though countries may find benefits in slightly different standards to achieve those outcomes. This focus on outcomes is already evident in the approaches taken by leading standards bodies: NIST notes that its "baseline product criteria for consumer IoT products are expressed as outcomes rather than as specific statements as to how they would be achieved,"[119] while ETSI says that its "provisions are primarily outcome-focused, rather than prescriptive, giving organizations the flexibility to innovate and implement security solutions appropriate for their products."[120] ETSI EN 303 645 already underpins national efforts in the United Kingdom, Singapore, Australia, Finland, Germany, India, Vietnam, and elsewhere, which goes a long way to ensuring a degree of uniformity in this space. As these countries have implemented national programs, they have supplemented the main ETSI EN 303 645 provisions with additional principles from other bodies, such as Singapore's Infocomm Media Development Authority (IMDA) and Germany's Federal Office for Information Security (*Bundesamt für Sicherheit in der Informationstechnik*, or BSI). While some variation among requirements is perhaps inevitable, it can risk becoming onerous for IoT vendors as additional provisions proliferate across jurisdictions. This highlights

[119] "Labeling for Consumer Internet of Things (IoT) Products," National Institute of Standards and Technology (NIST), February 2022. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.02042022-2.pdf.

[120] ETSI EN 303 645 – "Cyber Security for Consumer Internet of Things: Baseline Requirements."

the importance of encouraging countries to strive for similar outcomes and not just standards. Other IoT security frameworks may be referenced to bolster specific aspects of IoT security that are outside the scope of guidance found in standards such as ETSI EN 303 645, particularly those that extend beyond the device hardware and into the product's related software and apps. For instance, the App Defense Alliance has a framework that may be useful to reference while developing apps that are partnered with physical IoT products.

Similarly, governments must remain aligned on the products they consider "in-scope" for their IoT security efforts. ETSI EN 303 645, for example, covers "consumer IoT products that are connected to network infrastructure (such as the Internet or home network) and their interactions with associated services," and provides a non-exhaustive list of examples that includes:

> Connected children's toys and baby monitors; connected smoke detectors, door locks and window sensors; IoT gateways, base stations and hubs to which multiple products connect; smart cameras, TVs and speakers; wearable health trackers; connected home automation and alarm systems, especially their gateways and hubs; connected appliances, such as washing machines and fridges; and smart home assistants.[121]

Governments should consider how far to draw the line on systems, devices, and services with which IoT products connect—thinking about IoT cloud applications and other services that might fall under the scope of security baseline enforcement. For instance, the language in the UK's PSTI Bill—as written—excludes many IoT products from the scope of an IoT device, thus limiting the potential benefits of a mandated security baseline. As a starting point, governments should consider enforcing the baseline on all IoT products as well as on the systems and services on which IoT products depend to function. For example, if an IoT cloud application breaking would stop an IoT product from functioning, governments should consider including that in the scope of a default password mandate. Governments should delegate this task to the relevant cybersecurity standards agency and then embed the recommended definitional scope in legislation, regulation, and other requirements.

- **Recommendation 8: Governments and industry should review and, if necessary, update their respective tiers of standards every two years.** Technology changes quickly, and future efforts must ensure that guidance for security keeps up with the evolving security landscape. Further, there is a question of "moving goalposts"—once a government, for example, has success in requiring industry to meet the Tier 1 baselines, it should aim to raise the baseline even further through additional updates. Nonetheless, while standards can provide more specific guidance for organizations, governments should also consider mapping those evolving standards to a set of broader, desired security outcomes. Then, governments and industry should revisit and, if necessary, update their respective tiers of standards every two years, initiating update processes ahead of that two-year timeline such that the final updated guidance is ready for release at, or ahead of, the end of the two-year interval. Updating requirements each year with appropriate government, industry, and civil society consultation may require too much time and too many resources needed elsewhere, but without regular updates (e.g., every two years), IoT cybersecurity standards will become quickly outdated. On the international stage, standards bodies, including the ETSI and ISO, should continue to adapt guidelines as technological circumstances change and new information becomes available. This process should discard outdated and ineffective standards (or even contradict or undermine new security guidance), modify existing standards based on new technologies and risks, and consider adding new standards to each tier given the current rate of progress. To implement these changes into regulation, the UK's approach of empowering the DCMS secretary to define baseline security requirements—rather than "hard coding" them into legal text—provides an excellent model for replication. Law is extremely slow to change. However, if the appropriate agency or agencies receive the power to produce regulations and modify enforcement mechanisms within a stated scope of authority—and with appropriate government, industry, and civil society consultation—this would result in more regularly updated and thus more relevant and useful IoT security requirements.

[121] ETSI EN 303 645 – "Cyber Security for Consumer Internet of Things: Baseline Requirements."

- **Recommendation 9: Governments should develop additional guidance around the sunsetting phase of the IoT product lifecycle.** As illustrated in this report, many existing IoT security frameworks heavily skew towards the design, development, sale and setup, and maintenance phases of the lifecycle. Across best practice guidance, technical standards, and labeling and certification schemes, there is comparatively little IoT security focus on what happens when products are no longer receiving software security updates or must otherwise reach their end of life—and what manufacturers, vendors, and/or buyers should do to prepare for and handle that eventuality. This is a considerable oversight in the existing IoT security approaches. It also risks replicating a problem seen before with more conventional parts of the internet ecosystem, such as organizations needing to use old products and systems long after it is reasonably secure to do so (e.g., those running Windows 95). Governments should therefore develop additional guidance around the sunsetting phase, through their respective organizations designated with technical standard-setting. Producing this sunsetting guidance will take time and should not necessarily hold up the development and deployment of the minimum baseline tier of IoT security certification, but it is essential for addressing all parts of the IoT product lifecycle in a security approach.

These recommendations provide a sensible starting point to address the economic incentive issues that sustain consumer IoT's insecurity while promoting the core policy objectives of eliminating the most glaring vulnerabilities, harmonizing requirements across jurisdictions, encouraging greater prioritization of security by manufacturers, increasing consumer awareness, and making an overdue impact without further delay. Implemented and updated continuously, this would help drive towards a world in which IoT product manufacturers build in better security from the start—referencing many of the same sets of baseline security standards, roughly consensus and harmonized across jurisdictions—and every other actor in the supply chain follows, with manufacturers and vendors displaying understandable cybersecurity labels on products, retailers enforcing security requirements on those manufacturers and vendors, buyers looking to labels and other security guidance, and regulators ensuring that IoT security is better implemented across the entire device lifecycle.

Measuring Success

As with many cybersecurity issues, simple quantification of the problem is challenging. The discovery of a single vulnerability—whether in the product itself or in commonly used software packages—can mean that millions of IoT products are suddenly at risk. But methods to better understand and quantify IoT security risk are needed, both to better understand the nature of the problem and to measure the success of policy interventions and security standards. Several data points may prove helpful in enhancing understanding of the overall threat ecosystem presented to IoT products.

- *Information on the number of in-scope products:* One widely cited study from Transforma Insights, a market research firm, estimates that the number of active IoT products will grow to 24.1 billion by 2030, up from 7.6 billion in 2019, expanding on average 11 percent per year.[122]

- *Information on attacks:* After coming online, on average, an IoT product is probed within five minutes by tools that scan the web for vulnerable products, and many are targeted by exploits within 24 hours. Attacks on a simulated smart home, constructed by the UK consumer group called "Which?", reached 12,000 in a single week.[123] Kaspersky, a cybersecurity firm, maintains a network of "honeypot" devices to learn more about attacks, and measured 1.5 billion IoT attacks over the first half of 2021, up from 640 million over the same period a year prior.[124] Defining an "attack" can be another tricky question, with some definitions including activities that range from a relatively benign probe by a popular scanner tool to an all-out compromise of the device. It would perhaps be most fruitful to focus efforts on activities that hint at active malicious activity, such as brute-forcing attempts or attempts to employ remote code execution exploits.

- *Information on product insecurities:* Unit 42, a team of threat intelligence researchers at Palo Alto Networks, estimates that 57 percent of smart devices are susceptible to medium- or high-severity attacks, while 98 percent lack encryption in their communications, putting confidential personal information at risk.[125] Default manufacturer passwords, often the same for thousands of devices, provide some of the simplest entry points in the compromise of a device.

[122] "Global IoT market to grow to 24.1 billion devices in 2030, generating $1.5 trillion annual revenue," Transforma Insights, May 19, 2020, https://transformainsights.com/news/iot-market-24-billion-usd15-trillion-revenue-2030.

[123] "How a smart home could be at risk from hackers," Which?, July 2, 2021, https://www.which.co.uk/news/article/how-the-smart-home-could-be-at-risk-from-hackers-akeR18s9eBHU.

[124] "Kaspersky Detects 1.5B IoT Cyberattacks This Year," PYMNTS, September 3, 2021, https://www.pymnts.com/news/security-and-risk/2021/kaspersky-detects-iot-cyberattacks-double-last-year/.

[125] "2020 Unit 42 IoT Threat Report," Unit 42, March 10, 2020, https://unit42.paloaltonetworks.com/iot-threat-report-2020/.

In 2017, researchers at Positive Technologies found that five login/password combinations—support/support, admin/admin, admin/0000, user/user and root/12345—granted access to 10 percent of internet-connected devices.[126]

Measuring the impact of labels, standards, and legislation is harder still. In the UK, DCMS published cost-benefit analysis in parallel with the filing of the PSTI Bill. This report represents one of the more admirable efforts to quantify this risk and the potential benefits of intervention. But as the NCSC notes, analyzing the cost of intrusions specific to connected consumer products is very difficult today, as the user does not necessarily notice the attack, and the line between what is and is not an attack may be blurry from an outside observer's perspective.[127] Better methods to measure the impacts of policy interventions must continue to be the subject of research. An initial—and non-exhaustive—list of these metrics may include:

- Percent/number of products that meet various levels of security (as defined by ETSI/NIST/other frameworks).
- Percent of products using default passwords.
- Number of products infected with Mirai and other IoT malware.
- Percent of products sold whose company has a vulnerability reporting contact.
- Average response time / patch release time for critical vulnerabilities by product.
- Percent/number of unpatchable products in operation.
- Percent/number of products no longer receiving security updates in operation.
- Percent of customers who say they use product security as a key buying criterion.
- Percent of customers who say they trust the security of their IoT products.
- Number of IoT product vulnerabilities with high CVSS scores publicly disclosed (the assumption being at first a deluge of reporting as researchers start to focus on these products, and with time the number of found vulnerabilities decreasing).

What's Next for Labeling

Throughout the conversations with government and industry players, one point of worldwide consensus shines through: there is a solid appetite to adopt some sort of labeling scheme for consumer IoT devices. The benefits of such a scheme are plentiful. The ability to collect information on product security and having that information public offers exciting possibilities. Access to such information empowers purchasers and supports researchers and auditors in doing their work. IoT vendors have also recognized the benefits of labels from a marketing perspective, allowing them to use product security as a clearly articulated, understandable differentiator.

While the interest in labeling is there, the logistics are still lacking. There is a slew of details that need ironing out down the road. Getting them right is important for the IoT, and, as such, labeling merits future dedicated study. Plenty of questions exist around label design: How should it look? What information should it communicate? Beyond that are the bigger questions of how the system itself should work: Who could issue labels? What information would be needed to award a label? Where would that information be kept and stored, and how could it be accessed? Many details need workable answers—and there are lots of proposed ideas to sort through—before a labeling scheme can roll out on a global scale.

[126] Catalin Cimpanu, "15% of All IoT Device Owners Don't Change Default Passwords," BleepingComputer, June 19, 2017, https://www.bleepingcomputer.com/news/security/15-percent-of-all-iot-device-owners-dont-change-default-passwords/.

[127] DCMS, "Regulation of Consumer Connectable Product Cyber Security," RPC-DCMS-4353(2).

CONCLUSION

Inadequate security for consumer IoT products is just one of many difficult emerging technology issues that require global coordination among public and private sector actors. A range of parallel efforts exist to address wide-ranging digital challenges, such as protecting the privacy of personal data, addressing anti-competitive behavior by tech giants, and countering online misinformation. The steady march of technology means that poorly designed interventions risk irrelevance. Moreover, they leave the IoT more vulnerable to harm from the unintended consequences they should prevent.

Despite the perennially crowded global to-do list, reducing the threats from insecure consumer IoT products is overdue, attainable, and worthy of the world's attention. This report likely gives short shrift to the many benefits of consumer IoT, but fully realizing its potential requires addressing its worst failings. These deficiencies—rooted not merely in technology but, more so, in economic incentives—means that the IoT demands better policy intervention. A litany of proposals has at last turned into momentum behind some reasonable, consensus measures. As one interviewee said, "we cannot let the perfect become the enemy of the good."

From botnets that menace internet infrastructure to universal default passwords that allow hackers to invade user privacy, the impact on consumers is real, with risks that multiply in tandem with the number of connected devices. As Nathaniel Kim, Bruce Schneier, and Trey Herr contend, "these attacks are all the byproducts of connecting computing tech to everything, and then connecting everything to the Internet."[128] Unlike traditional appliances, which tend to degrade over predictable timescales and stop working individually, "computers fail differently."[129] They all work fine, until one day, the discovery of a vulnerability means finding a fix for all products of that particular model. As more and more things continue to become computers, they will increasingly fail like computers. The world needs processes, norms, and global standards that fit for this new reality.

[128] Nathaniel Kim, Trey Herr, and Bruce Schneier, *The Reverse Cascade: Enforcing Security on the Global IoT Supply Chain*, The Atlantic Council, June 2020, https://www.atlanticcouncil.org/in-depth-research-reports/report/the-reverse-cascade-enforcing-security-on-the-global-iot-supply-chain/.

[129] Bruce Schneier, "Security in a World of Physically Capable Computers, Schneir (blog), October 12, 2018. https://www.schneier.com/blog/archives/2018/10/security_in_a_w.html.

APPENDIX 1

Country-Specific Implementation Plans

This section discusses tangible, high-impact next steps that the UK, Singapore, Australia, and the United States can each take to bring about the global multi-tier system for IoT security detailed in our recommendations.

As noted earlier, this research seeks to capitalize on existing momentum, whether international or intranational. There are multiple viable paths for governments that are consistent with our vision to (1) rid the world of IoT's most glaring vulnerabilities and (2) harmonize international efforts to make it easier for firms to manufacture and sell products with even stronger security features. This implementation plan aims to nudge their approaches towards greater consistency, as opposed to calling for dramatic about-faces.

UK

Tier 1. Set the Baseline of Minimally Acceptable Security:

Of the four countries examined in this report, the UK is closest to creating a mandatory baseline for a broad range of IoT products sold in its market. The PSTI Bill, currently advancing in the House of Lords, will set minimum security requirements for manufacturers and couple them with potent enforcement mechanisms. By empowering the DCMS secretary to set these guidelines, this baseline can keep pace with technological change without the need to constantly rewrite legislation. The UK government should take the following actions:

- **Pass the legislation**. The most obvious and immediate next step is for parliament to enact the PSTI Bill. Thus far, the proposed law has made its way through the legislative process with its core provisions intact. While it does not address everything on the wish list of security advocates, it is an ambitious effort that lawmakers should approve. The House of Lords has recommended a sensible amendment that will also protect security researchers conducting legitimate vulnerability research from intimidation and lawsuits by manufacturers.[130] Given that the countdown for firms to comply with the new law begins one year after the bill receives Royal Assent—and that it has already been nearly nine months since its filing—consideration of further amendments should take into account the additional time they will add to the process.
- **Identify a regulator**. While the DCMS will define the cybersecurity provisions that manufacturers must abide by, it will not be the agency that enforces them. At the time of publication, the UK government had not publicly named the regulator responsible for enforcing the baseline product requirements. In its 2021 consultation, the DCMS sought recommendations on agencies well-positioned to serve in this role. Multiple respondents highlighted Trading Standards as a natural fit given its consumer protection role under Schedule 5 of the Consumer Rights Act 2015. Another was Ofcom, the UK's communications regulator.[131] The DCMS has also consulted with the Office for Product Safety and Standards in the Department for Business, Energy, and Industrial Strategy, another consumer product safety regulator.[132] This report does not have a specific recommendation as to the best-positioned agency to assume this role, but the government should announce this decision and begin to build out the key elements of its enforcement capacity.

Tier 2. Incentivize Above the Baseline:

Unlike the other three countries profiled in this report, the UK government has for now explicitly rejected the approach of device labeling, choosing to initially focus the bulk of its efforts on setting the first tier of a mandatory baseline. Despite the challenges with cybersecurity labels, the team views them as the best option for encouraging manufacturers to invest in greater security as well as providing consumers with accessible information. In partnership with NCSC, the DCMS should:

- **Provide "forward guidance" on provisions that it aims to mandate next**. Like a good central bank, the DCMS should provide predictability in its intended

[130] Alex Scroxton, "Lords Move to Protect Cyber Researchers from Prosecution, *Computer Weekly*, June 2022, https://www.computerweekly.com/news/252521716/Lords-move-to-protect-cyber-researchers-from-prosecution.

[131] "Government Response to the Regulatory Proposals for Consumer Internet of Things (IoT) Security Consultation." United Kingdom Department for Digital, Culture, Media & Sport (DCMS), February 2020, https://www.gov.uk/government/consultations/consultation-on-regulatory-proposals-on-consumer-iot-security/outcome/government-response-to-the-regulatory-proposals-for-consumer-internet-of-things-iot-security-consultation.

[132] "Proposals for Regulating Consumer Smart Product Cyber Security – Call for Views," United Kingdom Department for Digital, Culture, Media & Sport (DCMS), October 2020, https://www.gov.uk/government/publications/proposals-for-regulating-consumer-smart-product-cyber-security-call-for-views/proposals-for-regulating-consumer-smart-product-cyber-security-call-for-views.

future actions while remaining flexible to change in the face of new information. While the UK plans to begin with the so-called "top three" measures in its initial list of mandatory requirements, one of the key design principles of its approach is the ability to gradually ratchet up the baseline with new provisions. Through public announcements and meetings with industry, DCMS can telegraph where regulation is headed and allow security-minded firms to bring their products into compliance before the measures become mandatory. For starters, the DCMS should look to the World Economic Forum (WEF) statement that highlights two additional ETSI principles as the logical next steps: ensure that products communicate securely and safeguard personal data.[133] Other impactful measures could include a guideline requiring manufacturers to provide security updates for a minimum period consistent with the average length of time consumers use a product, which can vary by product category. The DCMS could go even further by publishing the planned effective dates of new security requirements years in advance. These provisions can change as cybersecurity threats and commercial considerations change.

- **Study the impact of cybersecurity labels in other markets and be prepared to reevaluate if they achieve results**. Thus far, research on cybersecurity labeling for smart devices remains largely limited to surveys about consumers' hypothetical willingness to pay more for products that have an indicator of greater security. Now that several countries have introduced labeling programs, users should begin to see "real world" data on their performance, both as it relates to changing consumer behavior and in addressing the downstream ills of insecure devices. If it becomes apparent that one or more of these labeling approaches are achieving success—or gaining traction as an international standard—the UK government should remain open to adopting it in its market.

Singapore

Tier 1. Set the Baseline of Minimally Acceptable Security:

While Singapore's CLS for consumer IoT is largely voluntary, it provides the regulatory infrastructure for a program that gradually expands to establish a baseline level of security for all devices. Internet routers sold in its market already must meet the provisions of the CLS Tier 1 label, which map directly to the UK's "top three" requirements that will be enforced with its proposed PSTI Bill. In consultation with IMDA and other partners, the CSA should:

- **Make the Tier 1 label mandatory for more product categories**. Internet routers have been a wise starting point: they have an outsize presence in today's botnets and can have security knock-on effects that threaten consumers' other smart home devices. Perhaps unsurprisingly, routers now account for over half of the CLS labels issued.[134] The CSA should consider the next highest priority product categories that will need to meet these minimum security measures, incorporating criteria like the (lack of) maturity in the category's cybersecurity features and the privacy risk to individuals if compromised. IP cameras, connected baby toys, and smart locks are strong candidates.

- **Add to the security provisions required as part of the Tier 1 label, especially those related to secure development practices**. CLS includes 76 security provisions, with roughly half required by one or more of its tiers, while the others are merely recommended. The first tier currently has 13 required provisions. Tier 2, which primarily concerns product lifecycle and secure development practices, has 17 required provisions—eight drawn from ETSI EN 303 645 and nine from the IMDA's IoT Cyber Security Guide. Over time, the CSA should aim to collapse the most impactful Level 2 requirements into Level 1, while removing those not seen as value-added. Alternatively, the CSA could keep the same provisions in each CLS level and gradually require that devices meet the second level. Since both CLS Levels 1 and 2 rely on manufacturer self-attestation, these changes should not require any operational changes in administering the program.

Tier 2. Incentivize Above the Baseline:

CLS has seen dramatic growth since the beginning of 2022, with the number of labels issued tripling during that timeframe. But the gains are not evenly distributed: of the 176 labels issued by CSA as of July 2022, 148 are at the Level 1 designation, an additional 16 are at Level 2, and 10 are for Level 4.[135] As mentioned earlier, many of the recipients of labels are internet routers, where the Level 1 label is mandatory. A key selling point of its multi-tier system is the ability to provide manufacturers with a reason to go above and beyond the bare minimum. To this end, CSA should:

[133] "IoT security: How We Are Keeping Consumers Safe from Cyber Threats," World Economic Forum, February 2022, https://www.weforum.org/impact/iot-security-keeping-consumers-safe/.

[134] CSA, Cybersecurity Labelling Scheme (CLS) Product List.

[135] CSA, Cybersecurity Labelling Scheme (CLS) Product List.

- **Conduct a review of the program's effectiveness in addressing the core problems associated with IoT insecurity and publish the findings**. As the country with the most mature cybersecurity labeling program, Singapore is in a unique position to gather information on the successes and challenges of this regulatory approach. How have consumers adapted their purchasing behavior since its launch? Has the number of insecure devices sold in Singapore decreased? What have been the challenges for firms? Have there been impacts beyond Singapore's borders? This review could also help improve the structure of the program. For example, it might review the fitness of the CLS tier structure. The inclusion of more levels makes sense if it adds to the range of choice for consumers and manufacturers to select the appropriate certification level that meets their needs. If no one selects it—currently the case for CLS Level 3—it is possible to simplify the scheme. The report's "Measuring Success" section includes some example metrics that could help gauge a topic that is notoriously difficult to quantify. The results will be helpful for Singapore, but just as critically, for the large number of countries and industry bodies that are experimenting with cybersecurity labels for IoT products.

- **Pursue an agreement with Germany for mutual recognition of cybersecurity labels**. Finland and Singapore's agreement shows that binary and multi-tier labeling approaches need not conflict. Germany, which recently launched its own binary label in January 2022, should also join the bilateral agreement between Singapore and Finland for mutual recognition. All three countries draw largely from the same list of ETSI EN 303 645 security provisions. Partnering with a market of Germany's size will add significant momentum for Singapore's approach to securing IoT, while reducing the burden of duplicate testing and certification for firms. This approach should be pursued for any country that adopts an IoT labeling program found to be largely compatible with the existing Singaporean program.

- **Consider measures to encourage broader adoption of the labeling scheme**. Anecdotal evidence suggests that many security-minded firms have been eager to participate in the program, but the CSA should continue to search for ways to increase its attractiveness. While the program will eventually need to generate revenue to cover its costs, CSA could extend the moratorium on application fees for an extended period, or even subsidize testing for devices at higher levels of security.

Australia

Tier 1. Set the Baseline of Minimally Acceptable Security:

Since the conclusion of its Call for Views in August 2021, Australia's DHA has been relatively quiet in public on its path forward for the regulation of consumer IoT. Whatever its ultimate action, it is evident that Australia aims to take a more hands-on approach than its past voluntary measures. To establish this minimum baseline, the DHA should:

- **Select a regulatory approach for mandating basic security requirements for devices sold in its market**. Australia has multiple approaches at its disposal and should continue to study the benefits and drawbacks of programs in the UK, Singapore, and elsewhere. The options it is most seriously considering are either a mirror image of the UK's minimum security standards or a four-level "graded shield" that appears very similar to Singapore's CLS. Australia's voluntary Code of Practice, which aligns with ETSI EN 303 645, should provide a strong foundation that will have prepared Australian businesses for more stringent enforcement.

- **If pursuing a minimum security standard, align its approach with the PSTI Bill's planned enforcement measures**. At a minimum, these measures should include the "top three," banning universal default passwords and mandating vulnerability reporting contacts and transparency on security updates. Preferably, it would also include additional provisions on securing personal data, encrypted communications, and minimum acceptable support periods for security updates. Currently, Australian Consumer Law does not require firms to adhere to any principles meant to reduce cyber risk, "only that they cannot make misleading or deceptive representations about the cyber security of their products."[136] This baseline could be achieved either through a new law, modeled on the UK's PSTI Bill, or an expansion of Australia's existing Consumer Law to incorporate protections against the most basic flaws in cybersecurity in its definition of "acceptable quality" and "fit for purpose."[137]

- **If pursuing a multi-level labeling approach, follow a strategy of gradual mandates by product category.** Given that it seems most drawn to a multi-tier label mirroring CLS, the clearest path for Australia is to follow Singapore's strategy and gradually mandate a tier 1 label by product type, beginning with high-priority items like internet routers. The labeling scheme should include a broad definition of in-scope prod-

[136] DHA, "Strengthening Australia's Cyber Security Regulations and Incentives."

[137] DHA, "Strengthening Australia's Cyber Security Regulations and Incentives."

ucts, drawing from ETSI's definition of smart devices. In addition to expanding mandates by product category, DHA can also raise the baseline over time by advancing along the other "axis" of incorporating more security provisions from higher security levels into its base tier.

Tier 2. Incentivize Above the Baseline:

The approach for incentivizing action to instill even greater security measures in its smart device market is highly related to Australia's method for enforcing its baseline. As DHA notes, these measures need not be mutually exclusive. To promote a higher tier of security, it should:

- **Select a cybersecurity labeling approach**. A study conducted by the Behavioral Economics Team of the Australian Government compared the effects of multiple label options on consumers, finding that "participants were more likely to choose a device with a cyber security label than one without a label, by 13–19 percentage points."[138] While the graded shield was most impactful, it found that "expiry labels were still effective" and "a high security level or long expiry date increased the likelihood of choosing a device."[139] Each of these options appears likely to have its own benefits and drawbacks, but it is time to choose one and move forward with it.

- **If pursuing an expiry date-label, study its effect and publish the findings**. If it follows through on this proposal, Australia would be the first to introduce a label that indicates the length of time manufacturers will provide security updates to the product. Studying this approach can help answer several questions about the impact of cybersecurity labels, particularly around the sunsetting phase. For example, are consumers incentivized to purchase devices at a discount that are about to go "off warranty"? As stated earlier, there is nothing wrong with national-level experimentation, as it can be beneficial in formulating new approaches that may be suitable for broader adoption.

- **If pursuing a "graded shield" label, agree to mutual recognition with Singapore and other participating countries**. The four-level labeling scheme that Australia appears likely to pursue bears many similarities with Singapore's CLS. In this case, the two countries should aim to bring their programs into close harmony, including the definitions of in-scope devices, the security provisions included in each tier, and the processes for self-attestation and third-party testing. Over time, the DHA should work with the CSA to ensure that the programs evolve together with consistency. Australia should then join the bilateral agreement with Finland for mutual label recognition, as well as a proposed agreement with Germany.

United States

Tier 1. Set the Baseline of Minimally Acceptable Security:

In comparison to other jurisdictions, the United States has preferred a less interventionist approach. There are two main exceptions: the two states that have enacted legislation to impose minimum security standards on IoT products, as well as the IoT Cybersecurity Improvement Act of 2020 which requires federal agencies to only procure devices that meet NIST security guidelines. In this context, the team recommends:

- **States should pass and enforce their own IoT security laws.** California and Oregon led the way but should expand their laws to focus on more specific guidance for organizations and manufacturers less versed in cybersecurity, rather than just focusing on concepts like "reasonable security." Ideally, they will do so in a way that does not lock in specific security measures into legal text but instead points toward another regulatory mechanism that more easily updates standards, such as the UK's approach of empowering an agency to maintain these standards, or points them to guidelines set for federal government agencies by NIST. More states should follow in their footsteps, putting forth IoT security laws that incorporate the standards outlined by the US government, as well as considering standards established by others around the world. The states that have implemented these laws should also study their impact. It is not apparent that any enforcement actions have yet occurred, which indicates one of two possible scenarios: all devices sold in their markets are now compliant, or enforcement has been insufficient. The latter seems more likely than the former.

- **The federal government should adopt the binary labeling approach proposed by NIST**. In NIST's February 2022 publication "Recommended Criteria for Cybersecurity Labeling for Consumer Internet

[138] "Stay Smart: Helping Consumers Choose Cyber Secure Smart Devices," Behavioural Economics Team of the Australian Government (BETA), March 2022, https://behaviouraleconomics.pmc.gov.au/sites/default/files/projects/beta-report-cyber-security-labels.pdf.

[139] BETA, "Stay Smart: Helping Consumers Choose."

of Things (IoT) Products," the organization recommends pursuing a binary labeling approach.[140] In this scenario, there would exist a single label stating that a product has met baseline security standards. Implementing the binary label would be a first step towards goals such as defining minimum security standards, creating and implementing a labeling program, and starting to broadcast to consumers what they should be looking for when purchasing IoT products. Among other details, this will require identifying an owner for the program, and the FTC would be the strongest candidate.

Tier 2. Incentivize Above the Baseline:

President Biden's 2021 Executive Order 14028 (Improving the Nation's Cybersecurity) directed NIST to design a labeling program for IoT devices, which should also serve as a mechanism to encourage the adoption of security measures that exceed the minimum baseline. The program's ultimate owner should:

- **Provide incentives for industry to obtain labels**. The US may look to Singapore and other countries that have adopted labeling programs to see how companies have been encouraged to participate in a labeling program and reach for higher tiers. Fee waivers for label applications may be a good way of incentivizing participation during the first few years of the program. Industry would likely react positively to some form of compensation for the third-party testing required to earn a higher label.

Provide liability protection for firms that pursue the higher, tier 2 security standards. Experts have indicated that many players in industry would be incentivized to pick up higher security standards in exchange for liability protections. There are various types of liability protections that may be considered here, and this report leaves such determination up to the regulatory body. The implementation of such liability protection may take the form of a law passed by Congress outlining these protections, or conversely may come in the shape of a publicly articulated approach by the FTC.

[140] NIST, "Recommended Criteria for Cybersecurity Labeling."

ABOUT THE AUTHORS

Patrick Mitchell is a consultant with the Atlantic Council's Cyber Statecraft Initiative. He recently graduated from the Master in Public Policy program at Harvard University's John F. Kennedy School of Government, where he studied issues at the intersection of emerging technology and global affairs, including a second-year thesis on international efforts to improve IoT security. Prior to this, he interned with the UN Secretary-General's Office and worked for several years as a consultant with Accenture, where he supported federal, state, and local government agencies on projects related to technology strategy and digital transformation. He also holds a B.S. in Management from Boston College.

Justin Sherman is a nonresident fellow at the Atlantic Council's Cyber Statecraft Initiative, where his work focuses on the geopolitics, governance, and security of the global Internet. He is also a senior fellow at Duke University's Sanford School of Public Policy and a contributor at WIRED Magazine.

Liv Rowley was an assistant director with the Atlantic Council's Cyber Statecraft Initiative under the Digital Forensic Research Lab (DFRLab). Prior to joining the Atlantic Council, Liv worked as a threat intelligence analyst in both the US and Europe. Much of her research has focused on threats originating from the cybercriminal underground as well as the Latin American cybercriminal space. Liv holds a BA in International Relations from Tufts University. She is based in Barcelona, Spain.

Atlantic Council | Board of Directors

The Atlantic Council is a nonpartisan organization that promotes constructive US leadership and engagement in international affairs based on the central role of the Atlantic community in meeting today’s global challenges.

1030 15th Street, NW, 12th Floor,
Washington, DC 20005
(202) 778-4952
www.AtlanticCouncil.org