ITIF | INFORMATION TECHNOLOGY & INNOVATION FOUNDATION

Why the United States and EU Should Seize the Moment to Cooperate on Cybersecurity Labeling for IoT Devices

NIGEL CORY | MARCH 28, 2024

The United States and European Union should work through the Trade and Technology Council to align their respective cybersecurity labeling programs for the Internet of Things rather than allowing IoT security to become another technical barrier to trade and technology cooperation.

KEY TAKEAWAYS

- The proliferating range of connected products comprising the Internet of Things (IoT)—from smart speakers to climate-control systems—is susceptible to relatively common security vulnerabilities that are increasingly exploited by cybercriminals.
- Many consumers do not feel well informed about the security of their devices and do not have a clear and easy way to find trustworthy security information. A standardized labeling system—with QR codes to access further information—would help address this need.
- The United States and European Union (EU) are both enacting cybersecurity labeling schemes for IoT devices. But different or conflicting requirements would create another technical barrier to transatlantic cooperation and trade.
- Transatlantic cooperation, via common technical standards, testing bodies, and a mutual recognition agreement, would be valuable because it would provide a common baseline for IoT cybersecurity and allow firms to only test once in order to sell in both markets.
- The United States and EU should seize the opportunity to address major gaps and differences in their respective IoT labeling programs—especially on technical standards and conformity assessments—while both programs are still in their formative stages.
- EU-U.S. cooperation on IoT cybersecurity labeling may seem like an esoteric technical issue, but successfully navigating it would provide a roadmap to align regulations for other new and emerging technology issues.

CONTENTS

INTRODUCTION

The United States and EU should align their respective approaches to cybersecurity labeling for IoT products—the U.S. Cyber Trust Mark and the EU's Cyber Resilience Act (CRA)—via technical standards and potentially a mutual recognition agreement (MRA).[1] This is exactly the type of early and proactive regulatory engagement that the United States and EU set out to do under the Trade and Technology Council (TTC). An aligned EU-U.S. approach would allow firms to only test once in order to comply with both systems. Cooperation on IoT cybersecurity labeling would avoid creating yet another regulatory point of conflict in the transatlantic trade and technology relationship. However, to make it happen, the United States and EU need to address major gaps and differences in their respective programs, especially on technical standards and conformity assessments. Cooperation on IoT cybersecurity labeling may seem like an esoteric technical issue, but if successfully navigated, it would provide a roadmap for future EU-U.S. efforts to align regulations for other new and emerging technology issues, as the core components (in terms of technical standards and conformity assessments) will be similar.

The United States and EU need to get past the public relations value of saying, "Yes, we should work together," and focus on ways to actually work together on new and emerging technology issues. After two-plus years of the TTC, tangible action is missing from a lot of the agenda. Cooperation on IoT cybersecurity is one way to rectify this. There's also a window of opportunity, as both the U.S. and EU IoT cybersecurity labeling programs are at a formative stage. The Biden administration should go into this initiative eyes wide open in terms of what MRAs do in practice, why they've historically been difficult to negotiate, and why the EU uses them. It should also recognize that MRAs take considerable political and institutional support and resources to be effective. The European Commission's recent push for MRAs may simply be an effort to pull one over its American counterparts, who may be unfamiliar with the challenges involved in negotiating and operationalizing MRAs. Hopefully this isn't the case and is instead part of a recalculation by the European Commission to use MRAs differently than in the past.

This report examines the U.S. and EU IoT cybersecurity labeling programs; how Singapore's program and MRAs for telecommunications equipment are reference points for potential

cooperation and how these should factor into potential EU-U.S. cooperation on IoT cybersecurity labeling; the role of technical requirements and standards in each side's respective programs; and what MRAs do in practice, why they're hard to negotiate, and why the EU uses them. In conclusion, it provides recommendations detailing the major challenges the United States and EU need to (individually and collectively) address to cooperate on IoT cybersecurity labeling.

A summary of the report's recommendations includes the following:

- The Biden administration should direct the National Institute of Standards and Technology (NIST) to prioritize IoT cybersecurity labeling, including through international cooperation. It should urge the Federal Communications Commission (FCC), as an independent agency, to do the same.
- The Biden administration should direct NIST and the FCC to plan to eventually use international standards to ensure the U.S. Cyber Trust Mark system becomes compatible with the EU's program. The Department of Commerce's IoT public-private advisory board would play an important role in advising on the development and use of international standards.
- The Biden administration and EU will need to negotiate an MRA to ensure products certified under the U.S.'s voluntary and binary IoT cybersecurity labeling system are accepted in the EU (and vice versa). This is similar to how Singapore has negotiated MRAs with Germany and Finland so that products certified under its voluntary, but tiered, IoT cybersecurity labeling system are accepted in both countries.
- The United States and EU should coordinate on the testing firms will need to complete (where required) to demonstrate conformity with their respective IoT cybersecurity labeling programs.
- The United States and EU should use IoT cybersecurity labeling as a roadmap for collaboration on other emerging technology issues.

BARRIERS TO EU-U.S. ALIGNMENT ON IOT CYBERSECURITY LABELING

The United States, EU, and other countries are enacting IoT cybersecurity labeling programs to help consumers make better decisions about the proliferation of connected products (e.g., smart speakers and doorbells, baby monitors, printers, smart refrigerators, microwaves, televisions, climate control systems, fitness trackers, and other connected devices) and to improve the cybersecurity of these products. IoT products are susceptible to a wide range of relatively common security vulnerabilities that are increasingly exploited by cybercriminals who are invading people's privacy and threatening national security. For example, Distributed Denial of Service (DDoS) attacks originating from insecure IoT devices increased fivefold from 2022 to 2023.[2] Some IoT products have even been shipped with malware in them.[3]

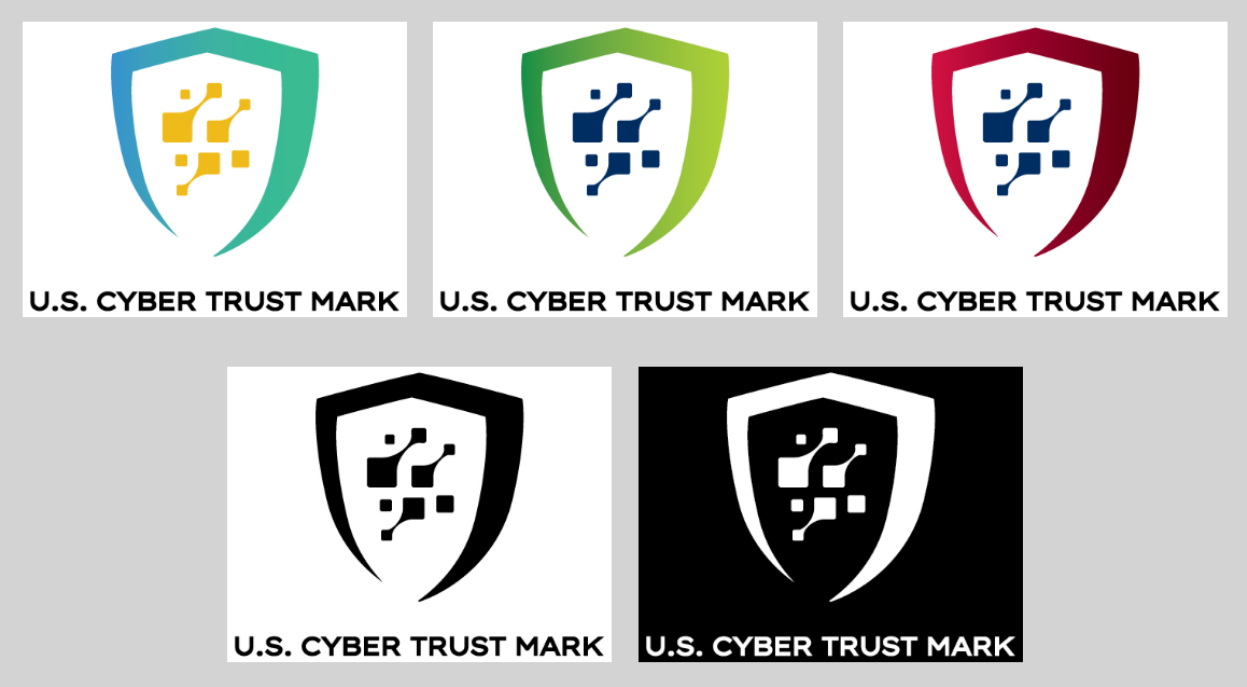
As the FCC states, consumers are concerned about the security of their IoT products, but they generally do not have access to convenient information on the security risks of these products prior to purchasing one.[4] *Consumer Reports* research finds that more than half of surveyed consumers do not feel informed about the security of the data collected by IoT devices and value information from manufacturers as to how their data gets used and stored, how long a product will receive security updates, and how good a manufacturer's security practices are—but they

have no consistent way to find that information and aren't sure if the info provided is trustworthy.[5] A label is intended to help address this by showing consumers that their products meet the cybersecurity standards of the IoT labeling program, which in turn strengthens the chain of connected IoT products in their own homes and as part of a larger national IoT ecosystem.

Labeling also supports improved enforcement. Instead of firms adhering to a vague standard of reasonable security they detail in their security and privacy policies, regulators can hold them accountable for doing what they say as required by the label's technical requirements. For example, the FCC stated that it "will pursue all available means to prosecute entities who improperly or fraudulently use the FCC IoT Label, which may include, but are not limited to, enforcement actions, legal claims of deceptive practices prosecuted through the U.S. Federal Trade Commission."[6]

In July 2023, the Biden administration first announced the U.S. Cyber Trust Mark, a voluntary cybersecurity certification scheme designed to better inform consumers that products have met baseline cybersecurity requirements (see figure 1).[7] On March 19, 2024, the FCC voted to (formally) create the U.S. Cyber Trust Mark.[8] It is due to start in late 2024. The U.S. Cyber Trust Mark is a binary system/label—products will either qualify to carry the label or not qualify (and thereby not be able to carry the label). It will be accompanied by a scannable code (e.g., QR Code) directing the consumer to more detailed information of the particular IoT product.

Figure 1: Examples of the U.S. Cyber Trust Mark[9]



The FCC manages the program, while NIST developed baseline criteria, and a pilot project, for the program, which includes product configuration, data protection, interface access control, software updates, and cybersecurity state awareness, among many technical issues.[10] The FCC's recent report and rule on IoT cybersecurity labeling outlines the same basic architecture they used for telecommunications equipment authorization: The specific requirements for products,

test methods, and certification are to be proposed by the U.S. Cyber Trust Mark's cybersecurity labeling administrators (CLAs) and provided to the FCC for approval through a "lead administrator."[11] The fact that CLAs are all likely to be potentially competing private sector entities is one of many challenges with the structure with regard to an MRA.

The goal is to be able to use the same label across different technologies beyond consumer IoT devices, such as drones. On January 11, 2024, Anne Neuberger (deputy national security adviser for cyber and emerging technologies in the Biden administration) announced the idea to pursue a U.S.-EU MRA on IoT cybersecurity labeling.[12] In contrast to other transatlantic issues, the United States has enacted a series of laws, regulations, and policies on IoT cybersecurity policies, including Executive Order 13800 on "Botnet Reporting and Roadmap," the IoT Cybersecurity Act of 2020 (which set minimum standards for federal IoT procurement), Executive Order 14028 on Improving the Nation's Cybersecurity, and the U.S National Cybersecurity Strategy.[13]

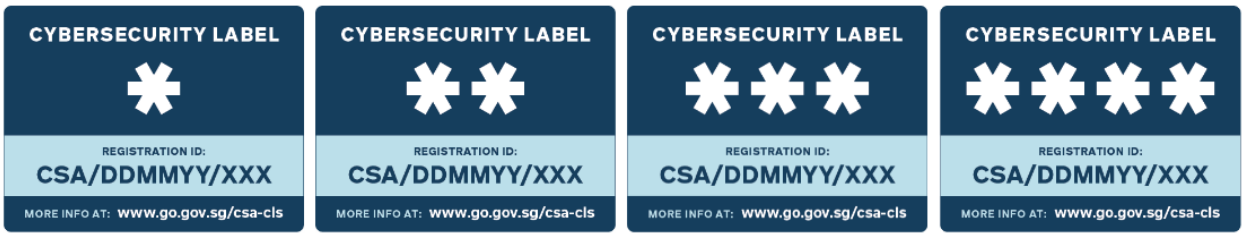
In 2024, the EU parliament is expected to finalize the CRA, which introduces cybersecurity requirements for the design, development, and production of hardware and software products across the EU.[14] It is a market access requirement, so it will be mandatory, not voluntary. It'll come into force over the next few years. The final list of products covered has not been finalized but is likely to include items covering both software and connected devices such as smart home devices, connected toys, and wearables. Manufacturers of products that are in conformance with the CRA will affix a CE mark (a label that certifies a product meets EU health, safety, and environmental requirements).

MODELS FOR TRANSATLANTIC COOPERATION

Lessons From Singapore: Positives and Pitfalls

Singapore is the model Biden administration officials had in mind when proposing U.S.-EU cooperation on IoT cybersecurity labeling, as Singapore had negotiated MRAs with trading partners (such as with Finland and Germany) to build recognition for its own Cybersecurity Labelling Scheme (CLS), launched in 2020 (see figure 2).[15] While CLS is voluntary for most products, new Internet routers sold in Singapore must meet the security requirements for its Level 1 label, requiring testing by third parties in certain situations.[16] As of March 19, 2024, 388 products had been certified.[17]

Figure 2: Singapore's four-tier IoT Cybersecurity Labeling Scheme[18]

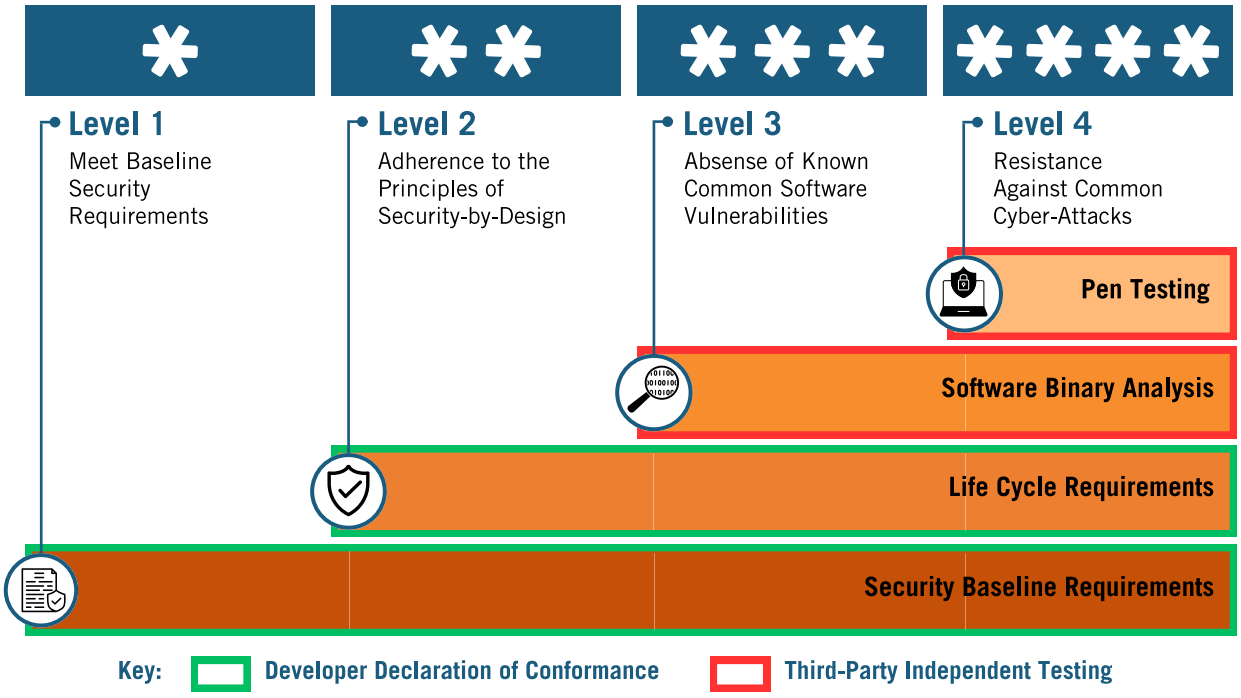


But Singapore's approach will be challenging for the United States to copy. CLS is a tiered system, while the U.S. Cyber Trust Mark is binary (see figure 3). For example, CLS level four is for products that have passed structured penetration tests and fulfilled requirements for all other levels. Their respective MRAs mean that Singapore's, Finland's, and Germany's systems recognize products certified at specific levels. Basically, Singapore's MRAs are focused on their

respective schemes' overall outcomes, as they essentially connect similar outcomes in terms of making a specific tier of its voluntary system meet the binary requirements of another country's scheme. It's unclear how this would work with a binary and voluntary system such as in the United States.

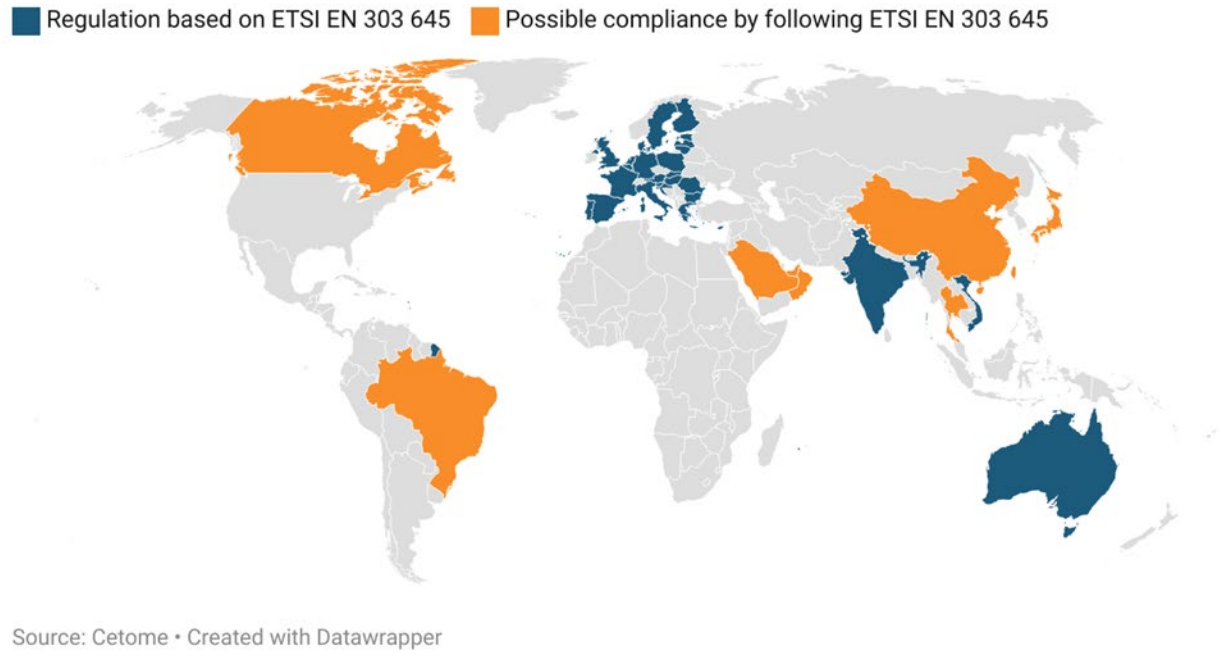
Singapore can more easily pursue MRAs as CLS uses the first global, and most broadly applicable, standard for consumer Internet of Things (known as EN 303 645, developed by the European Telecommunications Standards Institute (ETSI)).[19] Using the same standards provides an apples-to-apples comparison when looking at another country's technical requirements. The U.S. Cyber Trust Mark uses its own baseline technical requirements, and while it does reference this and other standards, it's unclear whether the U.S. program will evolve and directly use this or new international standards.

Figure 3: Singapore's Cybersecurity Labeling Scheme[20]



ETSI is one of three formally recognized EU standards bodies, which means firms that use its standards (called a "harmonized European standard") are in compliance with relevant EU laws (they are given a so-called presumption of conformity). Firms that use whatever standards ETSI eventually identifies or develops for the CRA will be automatically deemed to be in compliance with it. ETSI may be EU-based, but its membership includes many international firms, so its standards are often adopted internationally (see map 1). ETSI 303 645 will likely serve as the foundation of the EU CRA, as it already forms the basis for the U.K. Product Security legal regime and several other regulatory regimes in Finland, Germany, India, Vietnam, and Australia.

Figure 4: Countries with IoT cybersecurity programs aligning with the first globally applicable technical standard for consumer Internet of Things (ETSI Standard EN 303 645)



The Telecommunications Mutual Recognition Agreement

The United States and EU need an MRA to recognize testing arrangements so that tests done on one side of the Atlantic are accepted on the other. MRAs the United States negotiated for telecommunications equipment are the other key reference point for the Biden administration in proposing EU-U.S. cooperation on IoT cybersecurity labeling.[21] In general, the U.S. government is averse to negotiating MRAs. Also, the FCC's focus is on regulating the U.S. network rather than pushing for new international agreements. It'll take all relevant U.S. government agencies (e.g., the State Department, the Department of Commerce, NIST, and others) to develop international cooperation on IoT cybersecurity labeling, including through MRAs.

Enacted in 2000, the EU-U.S. MRA on telecommunications equipment has been successful. The goal of the telecommunications MRA was much the same as for the proliferation of IoT products—there were many cell phone models coming onto the market and it wasn't viable (or efficient) for the FCC to certify every single model, so they set up laboratory testing, third-party certifications, and MRAs with key partners to streamline the process to the same standard. The telecommunications MRA was a formative experience in showing the FCC and others how to ensure MRAs are effective. But it was not easy, as it takes ongoing institutional leadership, technical expertise, and dedicated resources. For example, there are three full-time NIST staff working on the U.S. telecoms MRAs to ensure accredited assessment bodies are up to standard, to update bodies with new information, and to engage with counterparts, among other activities.

TRANSATLANTIC COOPERATION MUST COVER TECHNICAL STANDARDS, CONFORMITY ASSESSMENTS, AND A MUTUAL RECOGNITION AGREEMENT

A U.S.-EU MRA on IoT cybersecurity labeling is a good idea. As part of an MRA, the EU would recognize U.S. organizations to test whether a product meets EU technical standards for IoT cybersecurity labeling (i.e., conduct a so-called "conformity assessment"). The FCC would do the same for qualified EU organizations to test FCC requirements, where relevant. Firms thus would not have to test their products again before going on sale in the EU or the United States. This sounds simple enough, but MRAs are anything but simple.

MRAs are complicated and difficult to negotiate, as they tend to deal with the respective countries' laws and regulations, which can vary significantly. MRAs also raise concerns about domestic regulatory enforcement and conflicting approaches to regulation. One former U.S. government negotiator called MRAs "my regulations apply," as parties, especially the EU, try to use them to enforce their regulations on the other side, which is problematic because countries regulate issues differently and there is often no one way to address an issue. Indicative of this, another former U.S. government official stated that, based on his time working on technical standards and conformity testing, the United States, in general, does not do MRAs, in part, as MRAs are fraught with a history of regulatory conflict between the United States and the EU. Both the Biden administration and the European Commission will need political will and leadership to overcome these challenges to ensure IoT cybersecurity regulations don't become another battlefield for regulatory conflict.

The technical standards the United States and EU use for their respective cybersecurity labeling programs are critical to potential cooperation. Without the same or similar standards, it's like comparing apples to oranges. NIST has taken a step in the right direction, as the baseline capability document for the U.S. Cyber Trust Mark references its baseline technical requirements with numerous reference standards. However, there's a significant gap between these baseline technical requirements and references and the "harmonized standards" the Biden administration's statement references.[22] Harmonized standards have a specific meaning. In the context of MRAs, harmonized standards effectively mean that both sides use the same technical requirements. At the moment, there's no indication that the United States and EU plan to use the same standards. Similarly, the Biden administration statement says the State Department is responsible for international engagement. Negotiating MRAs is typically a United States Trade Representative (USTR) responsibility (with support from other agencies such as NIST and the FCC). Either way, it is too early to begin MRA negotiations given that the U.S. and EU programs are in development. But this is a good thing, as it provides a window for the two sides to develop a way to work together via the use of international technical standards (and recognize their relevant testing bodies).

Technical standards for the EU's CRA are a work in progress. Ideally, the EU ends up using international standards, as doing so would make regulatory alignment with the United States (and others) much easier. Even before the CRA is enacted, the European Commission has sent a draft CRA standardization request to CENELEC (one of the other three European standards bodies) and the International Electrotechnical Commission's (IEC's) TC 65 committee (which developed the world's leading automation and control systems cybersecurity standard) so they could start the standardization process.[23] Ideally, the EU standardization process would use international standards as much as possible, such as ISO/IEC 27001 on information security

management, ETSI EN 303 645 on IoT consumer products, ETSI TS 103 732 on consumer mobile devices, and ETSI TS 103 848 on home gateway products, among others.[24] ISO/IEC 27404 on Cybersecurity labeling framework for IoT, currently under development, draws on both the Singapore CLS and ETSI standard and will provide a global framework for the future.[25]

The EU and United States should both use international standards to build regulatory and technical interoperability between their respective IoT cybersecurity labeling programs. This would allow firms to use one standard to build products that comply with technical requirements across multiple markets. The alternative—multiple, potentially conflicting country-specific standards—raises the cost and complexity of trade and regulatory compliance and undermines regulatory cooperation between countries.

The EU is prone to doing just this in using EU-specific standards as a technical (protectionist) barrier to trade to disadvantage foreign firms and products, even when there are international standards available. There are clear indications that protectionist technical standards are an emerging pillar of EU digital/technology sovereignty, including for artificial intelligence.[26] Unfortunately, the Biden administration has not raised these problematic standards developments with the EU at the TTC. The United States will have to push the EU to use international standards if it wants to build transatlantic cooperation on IoT cybersecurity. For their parts, NIST and the FCC would reference the same international standards as the EU in core requirement documents for the U.S. Cyber Trust Mark program. But again, there's no indication that NIST and the FCC are considering this.

The EU and United States should both use international standards to build regulatory and technical interoperability between their respective IoT cybersecurity labeling programs.

If the EU does not use international standards, IoT cybersecurity will become another point of regulatory conflict with the United States. In a scenario in which the EU does not use international standards, and a U.S. firm does not use the European standard, that firm would have to use a designated EU conformity assessment body (CAB), also known as a notified body, to test and show its product is in compliance with the CRA.[27] This represents a costly technical barrier to trade due to the EU's restrictive approach to testing requirements. EU CABs must be established in the EU, accredited by an EU-based accreditation body, and designated by the European Commission to test whatever regulatory requirements they've been deemed competent to test to. In contrast, the United States and many other countries allow third-party CABs to demonstrate compliance without necessarily having a sector-specific, government-to-government MRA in place, as doing so makes it much easier for firms from around the world to demonstrate compliance with standards in other markets.

The EU advocates for MRAs, as they work around a barrier the EU itself created by not accrediting and designating non-EU bodies to test under EU laws.[28] However, even there, it has not done much, which underlines the difficulty in negotiating MRAs. The EU's New Approach Notified and Designated Organizations (NANDO) list of accredited bodies, under MRAs, is pretty slim: Australia (2), Japan (0), New Zealand (1), Switzerland (30), and the United States (19), as well as those under its trade agreement with Canada (6).[29] U.S. government officials have asked EU member state accreditation bodies to accredit more international and U.S. bodies, which

they said they could do, but that they couldn't do without the European Commission's approval (which has not been forthcoming). Again, this highlights why it's critical for the EU (and the United States) to use international standards to avoid running into a battle over an MRA to designate U.S.-based testing bodies.

Thankfully, the FCC's testing structure for the Cyber Trust Mark (as outlined, but not yet finalized) may make it easier to pursue an MRA with the EU, especially if both sides work together on their respective testing arrangements as they're developed and implemented, given a traditional MRA essentially reflects respective regulators trusting each other's attestations that their testing bodies know how to test to each other's technical requirements. This is going to be difficult to do for IoT cybersecurity labeling, in part, as many of the testing bodies, processes, and standards don't yet exist and will be dynamic to address evolving threats. However, the details the FCC has outlined for its testing system are more rigorous than might otherwise be expected for a voluntary program.

Ironically, the FCC is creating a testing system that is similar to the EU's use of designated notified bodies. The FCC will select a lead administrator (LA) to carry out various administrative responsibilities, including reviewing applications and recognizing qualified and accredited CLAs to test and certify products. Similar to how it handles telecommunications products, the FCC will conduct post-market surveillance of the program and use this to instruct the LA and CLAs. This delegation of government authority is more direct than otherwise would be expected for a voluntary program and differs from what the FCC has done in other conformity assessment regimes. While it's unclear who the FCC will choose as the LA and CLAs, organizations that already assess telecommunication equipment are well positioned given their existing accreditations and experience. If these organizations do get the role as LA/CLAs, it would potentially make it easier for respective regulators to trust them under an MRA for IoT cybersecurity labelling given that they are a known and trusted actor.

The FCC is creating a testing system that is similar to the EU's use of designated notified bodies, which may make it easier to pursue an MRA with the EU if both sides work together on their respective testing arrangements.

The European Commission stated that MRAs were a priority at the most recent TTC (on January 30, 2024).[30] It also follows a recent European Center for International Political Economy paper that calls for an MRA on conformity assessment for machinery and electrical equipment.[31] Perhaps the EU's renewed focus on MRAs reflects a recognition that it needs to use them in a more creative, pragmatic, and timely manner to cooperate with like-minded partners on new and emerging technology issues. It may reflect the sum of the calculation that if the EU can't reform its problematic conformity assessment system, then it should ramp up the use of MRAs to build regulatory alignment on shared issues and to avoid irritants to transatlantic trade and technology cooperation. Or it could reflect a cynical effort by European Commission officials to dress up the same old tools in new garb as part of a self-interested play to push its regulations on an unsuspecting Biden administration. The EU might push for MRAs that suit its economic interests while disregarding regulatory cooperation and potential MRAs on issues of interest to the United States. The Biden administration should be wary and clarify the EU's position and plans for IoT cybersecurity cooperation.

RECOMMENDATIONS

There are five major challenges the United States and EU need to address (both individually and collectively) to cooperate on IoT cybersecurity labeling:

1. **The Biden administration should direct NIST, the FCC, the Department of Commerce, and other agencies to prioritize IoT cybersecurity labeling, including through international cooperation.** NIST may be reluctant to take on additional work on the issue as its agenda, budget, and staff are already stretched by other tech policy priorities. But if NIST and the Department of Commerce's IoT advisory board do not develop and execute a plan to eventually use international standards, it'll be difficult to eventually negotiate an MRA with the EU.

2. **The United States and EU should work to find a way for the EU system to accept products certified under the United States's voluntary system (as the EU system is mandatory).** This is somewhat novel. Singapore's IoT cybersecurity labeling program is also voluntary, and it has MRAs with Finland and Germany, but Singapore's system is tiered (the U.S. system is binary), which allows respective countries to recognize labels at certain levels with higher requirements.

3. It's unclear whether the FCC and NIST plan or are open to build on the baseline technical criteria of the U.S. Cyber Trust Mark system via the use of existing or new international standards. NIST's baseline criteria are not formal standards. The Biden administration should direct NIST, the FCC, and the Department of Commerce's IoT advisory board to engage and track relevant international standards discussions and commit to evaluating and eventually using them. This is critical for putting the U.S. Cyber Trust Mark in a position to eventually connect with the EU's (and others', such as Singapore's) program. NIST and the FCC could incorporate international standards by reference (whether via an agency publication or regulation) into the rulemaking process under the National Technology Transfer and Advancement Act of 1995 and the U.S. Office of Management and Budget Circular A-119.[32]

4. **The United States and EU should coordinate on testing requirements for their respective IoT cybersecurity labeling programs.** The United States and EU should talk about what they plan to do in regard to testing and develop a way (once the CRA is implemented) for the EU to accept tests from non-EU based testing bodies (e.g., the CLAs in the U.S. program). At the moment, it's unclear/unknown how the U.S. and EU programs will require firms to demonstrate compliance, whether via self- declaration, third-party certification via certified auditors, or third-party certification via government bodies.[33] This is critically important, as the EU is generally reluctant to designate testing bodies outside the EU.

5. **The United States and EU should use IoT cybersecurity labeling as a roadmap.** This is the type of proactive, early engagement they'll hopefully engage in for other new and emerging technology issues. Potential cooperation on artificial intelligence, quantum computing, cloud cybersecurity, and other new or emerging technology will all depend in part on the same common components; namely, international technical standards and conformity assessments.[34]

CONCLUSION

IoT cybersecurity labeling is not a headline-grabbing issue. But it represents the type of common-sense issue that the United States and EU (plus other countries) really should not have an issue working together on. However, a long history of transatlantic regulatory conflict makes cooperation anything but a sure thing. Despite this, there's a window to avoid repeating the past, as both the United States and EU are at an early stage in their respective programs and have a vehicle (the TCC) to help them focus on how to build bridges rather than wait for their respective regulatory systems to create barriers that, once created, are hard to remove.

Acknowledgments

The author wishes to thank Rob Atkinson, Stephen Ezell, Daniel Castro, and the IoT, technical standards, and conformity assessment experts who took the time to discuss IoT cybersecurity labeling. Any errors or omissions are the author's responsibility alone.

About the Author

Nigel Cory (@NigelCory) is an associate director covering trade policy at ITIF. He focuses on cross-border data flows, data governance, and intellectual property and how they each relate to digital trade and the broader digital economy.

About ITIF

The Information Technology and Innovation Foundation (ITIF) is an independent 501(c)(3) nonprofit, nonpartisan research and educational institute that has been recognized repeatedly as the world's leading think tank for science and technology policy. Its mission is to formulate, evaluate, and promote policy solutions that accelerate innovation and boost productivity to spur growth, opportunity, and progress. For more information, visit itif.org/about.

ENDNOTES

1. "Certification Mark – U.S. Cybersecurity Labeling Program for Smart Devices," U.S. Federal Communications Commission, https://www.fcc.gov/cybersecurity-certification-mark; "EU Cyber Resilience Act," European Commission, https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act.
2. Nokia, "Nokia Threat Intelligence Report finds malicious IoT botnet activity has sharply increased," press release, June 7, 2023, https://www.nokia.com/about-us/news/releases/2023/06/07/nokia-threat-intelligence-report-finds-malicious-iot-botnet-activity-has-sharply-increased.
3. Sead Fadilpašić, "These Popular Android TV Boxes are Reportedly Shipping Laced with Malware," *TechRadar,* May 21, 2023, https://www.techradar.com/news/these-popular-android-tv-boxes-are-laced-with-malware.
4. U.S. Federal Communications Commission, *FCC Fact Sheet: Cybersecurity Labeling for Internet of Things*, (February 22, 2024), https://docs.fcc.gov/public/attachments/DOC-400674A1.pdf.
5. Ibid.
6. This is similar to ITIF's recommendation (in 2016) for Congress to force companies to publish a security policy. Transparency supports accountability and oversight.

   Daniel Castro, "How Congress can fix 'internet of things' security," *The Hill*, October 28, 2016, https://thehill.com/blogs/pundits-blog/technology/303302-how-congress-can-fix-internet-of-things-security/; FCC Fact Sheet, "Cybersecurity Labeling for Internet of Things," Report and Order PS Docket No. 23-239, February 22, 2024, https://docs.fcc.gov/public/attachments/DOC-400674A1.pdf.
7. "Biden-Harris Administration Announces Cybersecurity Labeling Program for Smart Devices to Protect American Consumers," press statements, July 18, 2023, https://www.whitehouse.gov/briefing-room/statements-releases/2023/07/18/biden-harris-administration-announces-cybersecurity-labeling-program-for-smart-devices-to-protect-american-consumers/; Katerina Megas and Michael Ogata, "Our Quest: Advancing Product Labels to Help Consumers Consider Cybersecurity," National Institute of Standards and Technology, February 16, 2022, https://www.nist.gov/blogs/cybersecurity-insights/our-quest-advancing-product-labels-help-consumers-consider.
8. "FCC Creates Voluntary Cybersecurity Label Program for Smart Products," FCC, March 14, 2024, https://www.fcc.gov/document/fcc-creates-voluntary-cybersecurity-label-program-smart-products.
9. "Certification Mark – U.S. Cybersecurity Labeling Program for Smart Devices," FCC (used with permission), https://www.fcc.gov/cybersecurity-certification-mark.
10. National Institute of Standards and Technology, *Recommended Criteria for Cybersecurity Labeling for Consumer Internet of Things (IoT) Products*, (February 4, 2022), https://doi.org/10.6028/NIST.CSWP.02042022-2.
11. FCC, *FCC Fact Sheet: Cybersecurity Labeling for Internet of Things*.
12. Sara Friedman and Oliver Ward, "U.S., EU seek reciprocity agreement on Internet of Things standards," *Inside U.S. Trade*, January 16, 2024, https://insidetrade.com/daily-news/us-eu-seek-reciprocity-agreement-internet-things-standards.
13. "Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," U.S. Cybersecurity and Infrastructure Security Agency, https://www.cisa.gov/topics/cybersecurity-best-practices/executive-order-strengthening-cybersecurity-federal-networks-and-critical-infrastructure; "H.R.1668 - IoT Cybersecurity Improvement Act of 2020," https://www.congress.gov/bill/116th-congress/house-bill/1668; "Executive Order on Improving the Nation's Cybersecurity," May 12, 2021, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/; The Biden Administration, *National Cybersecurity Strategy*,

(March, 2023), https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.

14. Mark Young and Aleksander Aleksiev, "The EU's Cyber Resilience Act Has Now Been Agreed," Covington, December 1, 2023, https://www.insideprivacy.com/cybersecurity-2/the-eus-cyber-resilience-act-has-now-been-agreed.
15. Cyber Security Agency of Singapore, "Cybersecurity Labelling Scheme (CLS)," https://www.csa.gov.sg/our-programmes/certification-and-labelling-schemes/cybersecurity-labelling-scheme.
16. Ibid.
17. Cyber Security Agency of Singapore, "Cybersecurity Labelling Scheme (CLS) Product List," https://www.csa.gov.sg/our-programmes/certification-and-labelling-schemes/cybersecurity-labelling-scheme/cybersecurity-labelling-scheme-(cls)product-list.
18. Cyber Security Agency of Singapore, *Cybersecurity Certification Guide,* (2021), https://www.csa.gov.sg/docs/default-source/our-programmes/certification-and-labelling-scheme/cls/publications/csa-cybersecurity-certification-guide.pdf.
19. "Consumer IoT security," European Telecommunications Standards Institute, https://www.etsi.org/technologies/consumer-iot-security.
20. Cyber Security Agency of Singapore, *Cybersecurity Certification Guide*.
21. U.S. Federal Communications Commission, "Equipment Authorization - EU MRA," https://www.fcc.gov/general/equipment-authorization-eu-mra.
22. "Biden-Harris Administration Announces Cybersecurity Labeling Program for Smart Devices to Protect American Consumers," press release, July 18, 2023, https://www.whitehouse.gov/briefing-room/statements-releases/2023/07/18/biden-harris-administration-announces-cybersecurity-labeling-program-for-smart-devices-to-protect-american-consumers/.
23. Sarah Fluchs, "What cybersecurity standards will products in the EU soon have to meet?" *Medium,* August 31, 2023, https://fluchsfriction.medium.com/what-cybersecurity-standards-will-products-in-the-eu-soon-have-to-meet-590854ba3c8c; "TC 65 Industrial-process measurement, control and automation," The International Electrotechnical Commission, https://www.iec.ch/dyn/www/f?p=103:7:0::::FSP_ORG_ID,FSP_LANG_ID:1250,25; "ISA/IEC 62443 Series of Standards: The World's Only Consensus-Based Automation and Control Systems Cybersecurity Standards," The International Society of Automation, https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards.
24. "ISO/IEC 27000 family: Information security management," The International Standards Organization, https://www.iso.org/standard/iso-iec-27000-family; https://www.etsi.org/technologies/consumer-iot-security; European Telecommunications Standards Institute, *Technical Specification: Consumer Mobile Device Protection Profile*, https://www.etsi.org/deliver/etsi_ts/103700_103799/103732/01.01.01_60/ts_103732v010101p.pdf.
25. "ISO/IEC CD 27404 Cybersecurity IoT security and privacy," The International Standards Organization, https://www.iso.org/standard/80138.html.
26. Nigel Cory and Patrick Grady, "The EU's Approach to AI Standards Is Protectionist and Will Undermine Its AI Ambitions," (Center for Data Innovation, February 6, 2023), https://datainnovation.org/2023/02/the-eus-approach-to-ai-standards-is-protectionist-and-will-undermine-its-ai-ambitions/; Nigel Cory, "How the EU Is Using Technology Standards as a Protectionist Tool In Its Quest for Cybersovereignty" (ITIF, September 19, 2022), https://itif.org/publications/2022/09/19/how-the-eu-is-using-technology-standards-as-a-protectionist-tool/; Nigel Cory, "Europe Goes Protectionist on Global Technical Standards: The Example of

"Common Specifications" (ITIF, February 24, 2023), https://itif.org/publications/2023/02/24/europe-goes-protectionist-on-global-technical-standards-the-example-of-common-specifications/.

27. CABs are organizations designated by an EU country to assess the conformity of certain products before being placed on the market.
28. "Decision No 768/2008/EC of the European Parliament and of the Council of 9 July 2008 on a common framework for the marketing of products, and repealing Council Decision 93/465/EEC," https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32008D0768.
29. "Notified Bodies," European Commission, https://webgate.ec.europa.eu/single-market-compliance-space/#/notified-bodies/notified-body-list?filter=countryId:36,notificationStatusId:1.
30. Hannah Monicken, "EU official: Expanding mutual recognition a priority for next TTC," *Inside Trade,* January 24, 2024, https://insidetrade.com/daily-news/eu-official-expanding-mutual-recognition-priority-next-ttc.
31. Oscar Guinea and Vanika Sharma, "Calling on the EU-US Trade and Technology Council: How to Deliver for the Planet and the Economy" (The European Center for International Political Economy, January, 2024), https://ecipe.org/blog/call-on-the-eu-us-ttc/.
32. "Key Federal Law and Policy Documents: NTTAA & OMB A-119," NIST, https://www.nist.gov/standardsgov/what-we-do/federal-policy-standards/key-federal-directives.
33. FCC, *FCC Fact Sheet: Cybersecurity Labeling for Internet of Things*.
34. Nigel Cory, "Europe's Cloud Security Regime Should Focus on Technology, Not Nationality" (ITIF, March 27, 2023), https://itif.org/publications/2023/03/27/europes-cloud-security-regime-should-focus-on-technology-not-nationality/; Nigel Cory and Patrick Grady, "The EU's Approach to AI Standards Is Protectionist and Will Undermine Its AI Ambitions," (Center for Data Innovation, February 6, 2023), https://datainnovation.org/2023/02/the-eus-approach-to-ai-standards-is-protectionist-and-will-undermine-its-ai-ambitions/; Nigel Cory, "How the EU Is Using Technology Standards as a Protectionist Tool In Its Quest for Cybersovereignty" (ITIF, September 19, 2022), https://itif.org/publications/2022/09/19/how-the-eu-is-using-technology-standards-as-a-protectionist-tool/.