



COMPARATIVE ANALYSIS OF NATIONAL AND REGIONAL PRODUCT CYBERSECURITY FRAMEWORKS

TAYLOR ROBERTS
MARCH 2026



Comparative Analysis of National and Regional Product Cybersecurity Frameworks

March 2026

Author: Taylor Roberts

Taylor Roberts is a seasoned cyber and AI security policy expert with experience spanning academia, the US federal government, and the private sector, currently serving as Principal of AI Security Policy at Zenity. Previously the Global Director of Security and Trust Policy at Intel and a former Cybersecurity Advisor at the White House's Office of Management and Budget, Taylor works toward fostering collaboration with governments, industry, and standards organizations to strengthen the AI security cybersecurity ecosystem. He holds a Masters in International Affairs from UC San Diego.

Design: Taylor White

The Institute for Security and Technology and the authors of this report invite free use of the information within for educational purposes, requiring only that the reproduced material clearly cite the full source.

This report is written and published in accordance with the Institute for Security and Technology's [Intellectual Independence Policy](#). The authors are solely responsible for its analysis and recommendations. The Institute for Security and Technology and its supporters do not determine, nor do they necessarily endorse or advocate for, any of this report's conclusions.

Copyright 2026, The Institute for Security and Technology
Printed in the United States of America

About the Institute for Security and Technology

Uniting technology and policy leaders to create actionable solutions to emerging security challenges

Technology has the potential to unlock greater knowledge, enhance our collective capabilities, and create new opportunities for growth and innovation. However, insecure, negligent, or exploitative technological advancements can threaten global security and stability. Anticipating these issues and guiding the development of trustworthy technology is essential to preserve what we all value.

The Institute for Security and Technology (IST), the 501(c)(3) critical action think tank, stands at the forefront of this imperative, uniting policymakers, technology experts, and industry leaders to identify and translate discourse into impact. We take collaborative action to advance national security and global stability through technology built on trust, guiding businesses and governments with hands-on expertise, in-depth analysis, and a global network.

We work across three analytical pillars: the **Future of Digital Security**, examining the systemic security risks of societal dependence on digital technologies; **Geopolitics of Technology**, anticipating the positive and negative security effects of emerging, disruptive technologies on the international balance of power, within states, and between governments and industries; and **Innovation and Catastrophic Risk**, providing deep technical and analytical expertise on technology-derived existential threats to society.

Learn more: <https://securityandtechnology.org/>

Contents

- Executive Summary 1**
- Introduction 1**
- Methodology and Data Sources 2**
- Overview of the Global Product Cybersecurity Landscape 3**
- Product Security Requirements Overview 5**
- Comparative Analysis of Regulatory Approaches and Requirements 7**
 - Exclusion of Baseline Security Requirements 7
 - Scope of Covered Products and Systems 7
 - Incident Reporting and Vulnerability Disclosure Obligations 8
 - Software Supply Chain Transparency and SBOM Expectations 9
 - Product Lifecycle and End-of-Support Policies 10
- Penalties for Non-Compliance 10**
 - Implications for International Regulatory Harmonization 10
- Conclusion 11**

Executive Summary

This paper provides policymakers with a structured, comparative analysis of national and regional product cybersecurity frameworks and their implementation timelines. Drawing on a consolidated dataset of existing and emerging regulatory schemes, the paper identifies substantive areas of convergence and divergence across jurisdictions, with particular attention to scope, mandatory requirements, reporting obligations, and lifecycle expectations. The analysis is designed to support informed regulatory dialogue, enable follow-on international engagement, and provide a foundation for validation activities that advance global harmonization of product cybersecurity requirements.

While regulatory approaches differ in legal form and enforcement mechanisms, there is growing alignment around baseline security outcomes, incident reporting expectations, and software supply chain transparency. However, there is a notable lack of definitive implementation deadlines for U.S. regulations. Building on these findings, the paper offers policy-oriented recommendations for regulators seeking to reduce fragmentation while preserving national and regional policy objectives.

Introduction

The rapid proliferation of connected products across consumer, enterprise, and industrial contexts has elevated product cybersecurity from a technical consideration to a core regulatory concern. In contrast to enterprise cybersecurity that focuses on protecting an organization and its assets, product cybersecurity focuses on the security of devices, embedded systems, hardware, software, and more. Governments and regional bodies are increasingly adopting formal frameworks to establish baseline cybersecurity requirements for products, whether as a condition for sales to government or for market access writ large. While these initiatives share common objectives like risk reduction, transparency, and accountability, their requirements and timelines vary considerably, creating compliance complexity and potential barriers to international trade.

This paper seeks to systematically compare these frameworks and to highlight opportunities for alignment that may support future international harmonization efforts.

Methodology and Data Sources

This white paper is based on a comparative review of national and regional product cybersecurity frameworks captured in a structured dataset. The dataset consolidates publicly available information on laws, regulations, and government-led schemes that establish cybersecurity-related requirements for products placed on the market or procured by public authorities.

For each framework, the dataset records key regulatory attributes, including:

» **JURISDICTION**

- » The countries included in-scope for this analysis are: Australia, Canada, European Union, Japan, Singapore, South Korea, United Kingdom and United States.¹

» **MANDATORY, VOLUNTARY, OR PROCUREMENT-SPECIFIC STATUS**

» **PRODUCT AND SECTORAL SCOPE**

- » Categories for regulatory scope include: consumer IoT, enterprise software, industrial/operational technology systems, medical devices, automotive.

» **INCIDENT REPORTING & VULNERABILITY DISCLOSURE OBLIGATIONS WITH ASSOCIATED TIMELINES**

- » An incident is an occurrence that actually or imminently jeopardizes confidentiality, integrity, or availability.
- » A vulnerability is a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

» **COORDINATED VULNERABILITY DISCLOSURE (CVD) POLICY REQUIREMENTS**

- » A CVD policy defines how vulnerabilities will be handled and disclosed in coordination between the reporter and the affected organization.

» **SOFTWARE BILL OF MATERIALS (SBOM) REQUIREMENTS**

- » An SBOM is a formal record containing the details and supply chain relationships of various components used in building software.

» **PRODUCT LIFECYCLE AND END-OF-SUPPORT DECLARATION REQUIREMENTS**

- » These requirements ensure that there is a public acknowledgement of how and for how long a vendor intends to support a product's security

» **ENFORCEMENT STATUS, PENALTIES, AND COMPETENT AUTHORITIES**

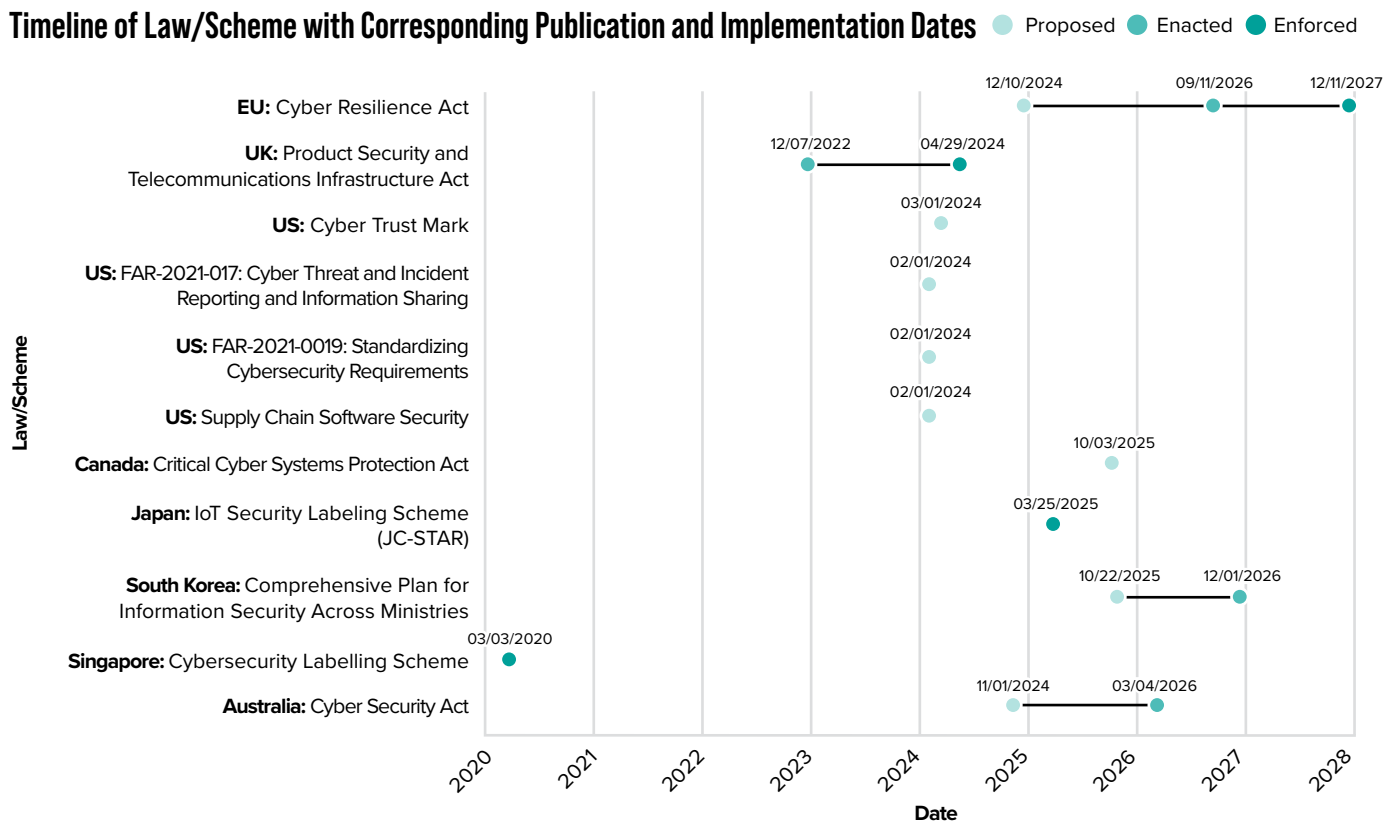
While enforcement dates or detailed implementation guidance are not yet finalized in all cases, qualitative indicators (e.g., “bill passed,” “rules adopted,” “program under development”) are used to assess regulatory maturity. The analysis emphasizes regulatory intent and practical compliance impact rather than official publication status.

¹ Specific regulations for each country can be found in the table in the [Product Security Requirements Overview](#). The United States has four separate pieces of policy that make up its product security framework.

Overview of the Global Product Cybersecurity Landscape

Across the surveyed jurisdictions, product cybersecurity frameworks can be grouped into three broad categories:

- » **COMPREHENSIVE MANDATORY REGULATORY REGIMES**
 - » [Cyber Resilience Act \(EU\)](#)
 - » [Product Security and Telecommunications Infrastructure Act \(UK\)](#)
 - » [Critical Cyber Systems Act \(Canada\)](#)
 - » [Cyber Security Act \(Australia\)](#)
- » **PROCUREMENT-SPECIFIC REQUIREMENTS (E.G., GOVERNMENT ACQUISITION RULES)**
 - » [FAR-2021-017: Cyber Threat and Incident Reporting and Information Sharing \(US\)](#)
 - » [FAR-2021-0019: Standardizing Cybersecurity Requirements \(US\)](#)
 - » [FAR-2023-02: Supply Chain Software Security \(US\)](#)
 - » [Comprehensive Plan for Information Security Across Ministries \(South Korea\)](#)
 - » [Cybersecurity Labelling Scheme \(Singapore\)](#)
- » **VOLUNTARY OR LABELING-BASED SCHEMES INTENDED TO INFLUENCE MARKET BEHAVIOR**
 - » [IoT Security Labeling Scheme \[JC-STAR\] \(Japan\)](#)
 - » [Cyber Trust Mark \(US\)](#)



[Click to view full **Product Security Requirements Overview**](#)

There is a clear divide between the regulatory-driven approach of Europe, Canada, and Australia, and the procurement incentivization of the United States, South Korea, and Singapore. It should also be noted that these latter approaches were originally voluntary or best practices, and were later extended to be procurement requirements.

Most of the approaches analyzed are either currently in effect (UK, Japan, Singapore, and Australia) or have a determined effective date (EU, South Korea). Canada and the United States are outliers. Their outlier status can be attributed to one of three reasons: either those regulations have missed their intended implementation deadline, lack a publicly stated effective date, or have been proposed but have not yet passed the regulatory process, even though administration officials have not withdrawn them altogether.

Product Security Requirements Overview

KEY

● Proposed ● Enacted ● Enforced

* Specified by manufacturer ** Updates required

Law / Scheme	Jurisdiction	Regime Type	Current Status	Date of Enforcement	Consumer IoT	Enterprise Software	Industrial / OT	Medical Devices	Automotive / Transport	VDP	Incident Reporting Required	IR Reporting Timing	Vulnerability Disclosure Required	Vuln Reporting Timeline	SBOM Required	End of Life	Penalties	Competent Authority
Cyber Resilience Act	European Union	Required	●—●—● Bill passed; Undergoing implementation	Vuln. reporting: 9/11/2026; Rest of bill: 12/11/2027	✓	✓	✓	✗	✗	✓	✓	24hr initial; 72hr follow-up	✓	24hr exploited vulnerability; 72hr follow-up; 14 day final	✓	*	Fines, market withdrawal	National Market Surveillance Authorities
Product Security and Telecommunications Infrastructure Act	United Kingdom	Required	●—● Bill passed; In force	4/29/2024	✓	✗	✗	✗	✗	✓	✗	N/A	✗	N/A	Implicit	✓	Up to £10M or 4% turnover	OPSS / DSIT
Cyber Trust Mark	United States	Voluntary	● Final rules adopted March 2024; Program still under development	TBD	✓	✗	✗	✗	✗	✗	✗	N/A	✗	N/A	✓	✗	Loss of certification	Federal Communications Commission
FAR-2021-017: Cyber Threat and Incident Reporting and Information Sharing	United States	Gov Procurement	● Comment period closed in February 2024	TBD	✗	✓	✗	✗	✗	✗	✓	8hr initial, 72hr follow-up	✗	N/A	✓	✗	Contract sanctions	CISA
FAR-2021-0019: Standardizing Cybersecurity Requirements	United States	Gov Procurement	● Comment period closed in February 2024	TBD	✗	✓	✗	✗	✗	✗	✓	8hr initial, 72hr follow-up	✗	N/A	✓	✗	Contract sanctions	CISA
FAR-2023-02: Supply Chain Software Security	United States	Gov Procurement	● Pending Notice of Proposed Rulemaking	TBD	✗	✓	✗	✗	✗	✗	✗	Included in other FAR cases	✗	N/A	✗	✗	Included in other FAR cases	CISA
Critical Cyber Systems Protection Act	Canada	Required	● Second reading and referral to committee on 10/3/2025	TBD	✗	✓	✓	✗	✗	✗	✓	24hr initial; 72hr follow-up	✗	N/A	✗	✗	Administrative fines or criminal charge	Public Safety Canada
IoT Security Labeling Scheme (JC-STAR)	Japan	Voluntary	● Program launched	3/25/2025	✓	✗	✗	✗	✗	✓	✗	N/A	✗	N/A	✗	**	Loss of certification	METI/IPA
Comprehensive Plan for Information Security Across Ministries	South Korea	Gov Procurement	●—● Policy passed, under implementation	by 2027	✓	✓	✗	✗	✗	Not yet	✗	N/A	✗	N/A	✓	✗	Fines up to 3-10% of sales for severe/repeated breaches, possible criminal charges	Office of National Cybersecurity
Cybersecurity Labelling Scheme	Singapore	Gov Procurement	● In force	Updated 05/2025	✓	✗	✗	✗	✗	✓	✗	N/A	✗	N/A	✗	**	Loss of label	CSA
Cyber Security Act	Australia	Required	●—● Bill passed 11/2024; Ransomware Reporting & Cyber Incident Review Board established 05/2025	3/4/2026	✓	✗	✗	✗	✗	Indirectly	✗	N/A	✗	N/A	✗	✓	Civil penalties	Department of Home Affairs

Comparative Analysis of Regulatory Approaches and Requirements

While all of these policies and regulations are intended to increase foundational cybersecurity measures for products within a country's jurisdiction, there remains significant divergence between the sorts of products considered in scope, the obligations of entities under scope, and the penalties for non-compliance.

Exclusion of Baseline Security Requirements

Evaluating the differences between specific security requirements across jurisdictions would offer those implementing the frameworks some clarity on how they differ or align with one another. Secure-by-design is a key theme throughout these regimes, as nearly all of the documents aim to ensure that products are designed, developed, and produced with an appropriate level of cybersecurity. Several countries, particularly those in Europe, use ETSI EN 303 645 as the base standard for secure-by-design requirements. The standard includes 13 key cybersecurity provisions, such as prohibiting universal default passwords, requiring a VDP, and mandating software updates within a specific timeframe. However, this paper does not attempt to compare discrete controls and requirements as, in most cases, these requirements are either still in development or not directly comparable due to the differences in product scope. It is difficult, for example, to compare identity and access management controls on microprocessors in the CRA, which are currently under refinement, to those in the Singapore Cybersecurity Labelling Scheme, which are finalized.

Scope of Covered Products and Systems

A central point of divergence across the frameworks is product scope. Many recent regulatory initiatives explicitly extend beyond consumer IoT to cover enterprise software, cloud-connected services, and industrial or operational technology systems. In contrast, voluntary schemes tend to focus narrowly on consumer-facing products, prioritizing transparency and consumer awareness.

On one end of the regulatory spectrum, the EU's Cyber Resilience Act expanded from only focusing on IoT devices to instead covering all products with digital elements. Product security, by this definition, encompasses "a software or hardware product and its remote data

processing solutions, including software or hardware components being placed on the market separately.” The EU CRA’s unique scope—the broadest of all product security regulations currently in the ecosystem—not only targets the component level, but also includes consumer, enterprise, and industrial/OT requirements. Other regulations, in comparison, either focus on consumer IoT (UK, U.S. Cyber Trust Mark, Japan, Singapore, Australia) or on enterprise software (FAR requirements in the United States). South Korea, meanwhile, intends to target both consumer and enterprise software, and Canada is looking toward enterprise software and industrial/OT.

For regulators, this raises important questions about boundary definitions, particularly where products transition across consumer, enterprise, and critical infrastructure contexts. International standards organizations have established definitions for each of these categories of products, but policymakers will need to consider which set of users they intend to impact before pursuing new regulations or expanding the scope of current requirements.

None of the regulations included in this evaluation cover medical devices or automotive devices. In most cases, this is because there are preexisting regulatory requirements in place to cover such devices, though it should be noted that aftermarket parts, non-type-approved components, software, and charging infrastructure may be subject to regulations like the CRA.

Incident Reporting and Vulnerability Disclosure Obligations

Vulnerability disclosure obligations and incident reporting policies are frequently treated as core regulatory expectations. Determining their prioritization across the policy ecosystem can therefore highlight potential harmonization opportunities.

Vulnerability reporting is a relatively nascent regulatory push; currently, only the CRA requires the reporting of actively exploited vulnerabilities. However, other regimes address vulnerabilities as a part of product security regulations. Regulations in the EU, UK, Japan, and Singapore explicitly require those subject to their requirements to publish a coordinated vulnerability disclosure (CVD) policy. Though not yet to the point of explicit requirements, South Korea has indicated it is moving in this direction and Australia currently requires that “manufacturers publish a means to report security issues,” though not necessarily in a formal CVD policy.

Outside of vulnerability disclosure obligations, several of the product security regulations require cybersecurity incidents be reported to a designated national authority. The EU, FAR cases in the United States, and Canada require incident reporting, though they diverge on their reporting timeline. The EU and Canada require an initial report within 24 hours of an incident being discovered, with a more detailed report required in 72 hours. The United

States, on the other hand, is set to require initial reporting within 8 hours, followed by the same 72-hour more detailed report. These differences in reporting timelines will complicate cross-border incident management and suggest an opportunity for greater alignment around common reporting principles.

Notably, some regulations require incident reporting even if the incident occurs on the product owner's network, but the impact to the product is still unknown. The CRA, for example, requires reporting if an incident "negatively affects or is capable of negatively affecting the ability of a product with digital elements to protect the availability, authenticity, integrity or confidentiality of sensitive or important data or functions." This could trigger a reporting requirement, even if the incident occurred on a corporate business network, rather than in a production environment. Similarly, the U.S. FAR Council draft rule requires Federal contractors to report incidents impacting their networks, regardless of whether the incident in question directly impacts a product sold to the government.

Finally, the EU CRA leaves some ambiguity around incident reporting frequency depending on the impacted organization's level of awareness. Consider a scenario where a manufacturer reports an incident stemming from an exploited vulnerability in their product. That same vulnerability could trigger multiple incidents. In some cases, the product owner may not even be aware of the impacted entity, whether because the incident was identified and reported by an integrated device manufacturer or because it was identified and reported by another company in the supply chain. As a result, a single vulnerability could generate numerous incident reports filed by multiple supply chain actors, each reporting based on their own awareness of the incident. This dynamic will likely result in significant overreporting and will require ENISA to triage incoming reports to assess the full extent of the vulnerability or incident's impact. More broadly, this example highlights the complexity of designing a regulatory regime that tracks incidents and vulnerabilities across a broad spectrum of product types.

Software Supply Chain Transparency and SBOM Expectations

Software supply chain risk management, including the use of software bills of materials, is an emerging area of regulatory convergence. While some frameworks impose explicit SBOM requirements (EU, U.S. Cyber Trust Mark, U.S. FAR Cases, and South Korea), others establish implicit expectations through broader risk management or documentation obligations (UK). Notably, other regimes did not include an SBOM expectation at all (Canada, Japan, Australia). Regulators therefore face the challenge of balancing transparency objectives with concerns around administrative burden, confidentiality, and the operationalization of SBOM data.

Product Lifecycle and End-of-Support Policies

Several product security frameworks include product lifecycle support. The CRA has a specified support window of 5 years that can be superseded by a manufacturer's declared support window. This reliance on a public declaration of product support is echoed in Australia and the UK, while Singapore's label is only valid while the product is under support. Other regimes do not include product lifecycle as a component of their regulations.

One aspect of this product lifecycle requirement that warrants further study is what constitutes a change to the product significant enough to trigger a new product support window. Europe is currently evaluating this question as part of the CRA implementation process, while other governments have yet to address this versioning issue. This distinction matters, as it will likely impact how frequently a product is subject to regulatory evaluation, whether through third party assessment, self-attestation, or another mechanism.

Penalties for Non-Compliance

The penalties for non-compliance vary across these regimes. Given that many of these schemes are voluntary in nature, non-compliance would simply mean a revocation or denial of the label or designation (U.S. Cyber Trust Mark, Singapore, Japan). Similarly, for those requirements that are mandatory in order to qualify for government procurement, non-compliance would mean either a failed tender or possible removal from government networks and ecosystems (U.S. FAR Cases). Several other frameworks include monetary penalties: the UK requires up to £10M or 4% turnover; the EU requires €15 million or 2.5% turnover; Australia's is AUD\$50 million, three times the benefit obtained, or 30% of adjusted turnover; and South Korea will implement fines up to 3 to 10% of sales for severe or repeated breaches, with possible criminal charges depending on the severity of the negligence.

Indeed, these product markets are inherently global. It remains to be seen whether manufacturers wind up being penalized in multiple jurisdictions for failures to meet cybersecurity requirements. In evaluating the efficacy of their frameworks, policymakers should consider whether the nature of the enforcement mechanism leads to materially different product cybersecurity outcomes when compared to other jurisdictions.

Implications for International Regulatory Harmonization

By categorizing the components that comprise product security regimes across a number of key geographies, this report provides a grounded framework for exploring the differences

in national and regional approaches. This report provides policymakers with a primer for international dialogue on harmonization or reciprocity and mutual recognition in product security. If countries can articulate that their regulations will address, for example, product scope, incident and vulnerability reporting, vulnerability disclosure, product lifecycle, and regulatory incentivization, then determining the specific requirements, timelines, thresholds, penalties, etc. within these categories can be discussed as a matter of national prioritization. Without agreement on what issues need to be addressed, however, it will be very challenging to harmonize the specific requirements across regimes.

Conclusion

As product cybersecurity regulation continues to expand, comparative analysis provides a critical foundation for informed international dialogue. By identifying both convergence and divergence across existing frameworks, stakeholders can better target harmonization efforts that enhance security outcomes while minimizing regulatory fragmentation and duplicative compliance activities.



INSTITUTE FOR SECURITY AND TECHNOLOGY

www.securityandtechnology.org

info@securityandtechnology.org

Copyright 2026, The Institute for Security and Technology