

ENDORSED BY:

AKAMAI

ALLIANCE FOR
AUTOMOTIVE INNOVATION

AMERICAN CHAMBER OF
COMMERCE IN JAPAN

AT&T

CABLELABS

CISCO

CONSUMER TECHNOLOGY
ASSOCIATION

COUNCIL TO SECURE THE
DIGITAL ECONOMY

CTIA

CYBERSECURITY
COALITION

ERICSSON

IBM

INFORMATION
TECHNOLOGY
INDUSTRY COUNCIL

INTEL CORPORATION

JAPAN ELECTRONICS
AND INFORMATION
TECHNOLOGY INDUSTRIES
ASSOCIATION

LUMEN TECHNOLOGIES

NCTA – THE INTERNET &
TELEVISION ASSOCIATION

NTT

OPEN CONNECTIVITY
FOUNDATION

ORACLE

SAMSUNG ELECTRONICS

SAP

TELECOMMUNICATIONS
INDUSTRY ASSOCIATION

TELEFÓNICA

U.S. CHAMBER OF
COMMERCE

USTELECOM | THE
BROADBAND ASSOCIATION

VERIZON

IoT Security Policy Principles

Policy Considerations Building on the C2 Consensus on IoT Device Security Baseline Capabilities



CSDE 

Council to Secure the
Digital Economy

Introduction

SINCE CSDE[†] PUBLISHED its C2 (“Convene the Conveners”) Consensus document in September 2019, the societal and economic benefits of the Internet of Things (IoT) have only increased, thanks to the explosive growth of the IoT itself. This technological evolution is being fueled by enhanced broadband connectivity, new product innovations and the growing role of digital infrastructure across all domains. With the growth of the IoT, however, comes an increase in the diverse and rapidly changing security threats. The IoT has a complex nature in terms of multiple sectors, business models, attack surfaces, threat vectors, technical infrastructure, and risk environments. In combination with its widespread deployment across networks and rapid growth, these elements of complexity drive the need for effective security solutions. These concerns have sparked numerous cross-industry, consensus-driven approaches and standards efforts aiming to promote the security and the resilience of the IoT Device ecosystem, and related domains.

This diversity of efforts in addressing IoT security challenges was an important motivator for CSDE’s C2 Consensus project. The C2 effort convened a broad range of technical experts from many groups to develop a common set of technical security guidelines. This effectively created a consensus ‘baseline’ of connected device security capabilities. These consensus capabilities were then mapped to equivalent capabilities defined in other important standards and guidelines, tying the various standards together in one document.¹ This mapping also proved how closely the various “minimum expectations” requirements around the globe can be aligned.

The C2 Consensus was recognized and has been cited by other consensus-driven reports and standards such as the National Institute of Standards and Technology (“NIST”)’s NISTIR 8259/8259A,² and draft ISO/IEC 27402³ (which is currently in development under the management of ISO/IEC’s Joint Technical Committee 1, Specialist Committee 27, or “JTC1 SC27”). A follow-on technical standard, CTA-2088 *Baseline Cybersecurity Standard for Devices and Device Systems*, was released in November 2020. CTA-2088 provides sufficient rigor and specificity to enable conformity assessment.⁴ CTA-2088 directly maps to the exact capabilities listed in the C2 Consensus and defines specific engineering requirements for those capabilities. This kind of clear expert guidance to industry and government on securing new IoT devices has potential to raise the market’s expectations for security and to advance global policy harmonization.

Policymakers and industry as a whole recognize the critical role of the C2 effort and other consensus-based efforts in promoting security—in a manner that is interoperable, scalable, measurable, and globally applicable. Similarly, the importance of this security for the IoT ecosystem is recognized by policymakers as they contemplate various regulatory and policy approaches. Such approaches may include elements of legislation, certification, labeling, procurement and “baseline”/security controls requirements.⁵ The technology and policy community has developed principles and positions on IoT security, seeking to inform policy efforts as they are being developed.

CSDE offers this document summarizing these core IoT Security policy principles. While not the product of CSDE itself, we highlight them to show the broad agreement on key security approaches among leading organizations across the information and communications technology (ICT) sector. In consolidating these efforts, this document can serve as a resource and further highlight how industry consensus-driven efforts on baseline security capabilities for IoT Devices efforts, such as the C2, can beneficially inform the conversation. The document is not an exhaustive view of these principles, which may evolve with time, but rather serves to highlight the common themes.

[†] The Council to Secure the Digital Economy (CSDE) brings together companies from across the information and communications technology (ICT) sector to combat increasingly sophisticated and emerging cyber threats through collaborative actions. CSDE is coordinated by USTelecom and the Consumer Technology Association (CTA).

Commonly Accepted IoT Security Policy Principles

To preserve the benefits of the IoT to consumers, organizations, and the global computing infrastructure, public policies should encourage innovation and competition, as well as accelerate secure, scalable, and interoperable IoT deployment. These proposed policy principles can further inform policymakers looking to adopt mechanisms to govern IoT device security.

1. The complexity of the IoT ecosystem merits a design neutral, interoperable approach to regulation that promotes the flexible adoption of consensus-based standards

The IoT encompasses a variety of sectors with different use cases ranging from global infrastructure operations and industrial control systems to individual consumers. As such, the threat models and risk vectors for IoT devices are not homogenous and vary in complexity and sensitivity from device to device and where and how it is deployed. As the technological landscape, economic models and attack surface develop, new security challenges arise. From a regulatory perspective, the IoT can rely on existing security policy principles developed and applied more broadly in the area of security: *harmonization (avoiding fragmentation), technology/design neutrality, and reliance on flexible adoption of open, consensus-based reports and international standards*. These principles will ensure policy and regulatory frameworks can comport with evolving technical landscapes in a flexible manner, while promoting innovation and certainty for businesses developing IoT products.

Overly prescriptive laws and regulations (e.g., non- design-neutral approaches) have proven to be a poor fit for the dynamic technology environment. This is so even where the policies include universally applicable baseline requirements. Instead, policymakers should rely on consensus-driven standards-based approaches, both global and domestic, that can adapt to dynamic and complex technological environments. They should also encourage the flexible adoption of standards that can be applied to different industry verticals (e.g., ISA/IEC 62443, compared to horizontal standards, such as CTA-2088 or ISO/IEC 27402 (in development)). Applying these principles across the IoT is key as it further interacts with the broader IT ecosystem encompassing cyber-physical systems.

2. Policies should leverage existing consensus-based standards and best practices on IoT Security and avoid the fragmentation inherent in regional approaches

Rather than outlining prescriptive requirements in regulation or legislation, policies and frameworks should encourage the flexible adoption of consensus-driven, widely adopted standards and best practices, including internationally. Unlike government-mandated regulations or policies, which may be static and become quickly outdated, consensus-driven standards and practices that are developed with broad industry and expert contribution and are routinely updated are better suited to keep pace with advances in the IoT. Policymakers should further consider frameworks that create proper incentives (legal, such as liability protections and safe harbors) to foster the adoption of such standards by industry, and avoid divergence from these key widely adopted best practices.⁶

A number of these consensus-based processes have been developed to establish baseline IoT Security requirements/capabilities applicable horizontally across IoT sectors. These efforts include:

- ▶ The C2 Consensus on IoT Device Security Baseline Capabilities, https://securingdigitaleconomy.org/wp-content/uploads/2019/09/CSDE_IoT-C2-Consensus-Report_FINAL.pdf⁷
- ▶ CTA-2088, Baseline Cybersecurity Standard for Devices and Device Systems, <https://shop.cta.tech/products/baseline-cybersecurity-standard-for-devices-and-device-systems-cta-2088>
- ▶ NISTIR 8259/8259A, IoT Device Cybersecurity Capability Core Baseline, <https://doi.org/10.6028/NIST.IR.8259A>
- ▶ Draft ISO/IEC 27402 (in process) (Cybersecurity – IoT security and privacy – Device baseline requirement), <https://www.iso.org/standard/80136.html>


Multiple standards have already been or are currently being developed for different industry verticals.

Policies should make consistent use of clear definitions based on such consensus efforts to avoid fragmentation, including of key concepts such as “Device”, “IoT Device” and “IoT device Manufacturer.” For example, as clarified in NISTIR 8259A, an IoT Device, “ha[s] at least one transducer (sensor or actuator) for interacting directly with the physical world and at least one network interface...Components of a device, such as a processor or a sensor that transmits data... that cannot function at all on their own are outside the scope.”⁸ An IoT device is not a general-purpose computing device (such as personal computing system, laptops, or smart mobile), as the computing and security capabilities and concerns differ greatly and are better addressed under other frameworks.⁹

Given the inherently global and interconnected nature of ICT supply chains—as well as the IoT embedded nature of the IoT ecosystem and the various systems that interact with it—there should be a focus on facilitating interoperability and avoiding duplicative and fragmented security requirements. Interoperability promotes security, future innovation and facilitates market access to security solutions developed globally. Conversely, locally or regionally fragmented approaches risk hindering security, technological development, and competition, and may cause product cost increases and delays in critical segments. Fragmentation could impede a market access to security innovations by local and smaller-scale, manufacturers who are less able to compete in global markets due to high regulatory and compliance costs. Further, such costs are ultimately borne by consumers and end users and risk dampening demand for innovative new products. In contrast, standards-driven approaches facilitate interoperability across IoT ecosystems, foster innovation and technology development, improve international collaboration, serve as the basis for market-tested attestation and certification frameworks, and enable cost-effective security solutions.

3. Policies should take device risk management profiles into account, rather than adopting a one-size-fits-all approach

Considering the incredible variety of the IoT—which includes wearable fitness trackers, industrial control systems, consumer security cameras, medical devices, enterprise lighting systems and more—a single technical requirement is unlikely to secure all systems in an efficient manner. The risk management profile for a fitness tracker is simply different from that of a thermal sensor on a power plant. Setting the same requirements for fitness trackers as for industrial controls systems leads to requirements that are either over- or under-specified. Cybersecurity expert working groups are familiar with this challenge and use risk-based analysis to appropriately scale effort.¹⁰



Similarly, policies and frameworks should draw from established international standards practices to assess risk and determine appropriate mitigations. These practices outline considerations for how risk analyses should be conducted and explain that the applicability of IoT security capabilities depends on the “on a variety of factors—from device complexity, deployment environment (managed or unmanaged), risk management profile, use case and context.”¹¹

The risk analysis approach recognizes that device manufacturers may not have all the information concerning the use case and environment in which the IoT device will be deployed. Moreover, for certain sophisticated use cases, such as industrial IoT, some security capabilities could be provisioned and enabled by end-users.¹² The limitations manufacturers face in predicting how IoT devices will be used and deployed in a changing environment means that it is especially challenging for them to anticipate the impact of potential attacks.

Because the security risks to the IoT differ drastically based on such factors, a one-size-fits-all policy approach is ill-suited to address the rapidly evolving threat landscape. Rather, policies that allow for the flexible adoption of standards based on the risk management profile¹³ of particular industry verticals and enterprises will enable manufacturers to better identify and remedy security threats that arise. There may be domains (such as automotive) that are regulated under a specific government authority or set of regulations, that take into account such standards and profiling, and should be excluded from general IoT security proposed regulations or policy.

This approach may be combined with Baseline security, which establishes a minimum level of security capability for all devices, applied based on a risk-assessment, but does not attempt to address all needs of device security. Baseline is a starting point that provides a certain minimum, and with risk-based assessment one can determine what further steps should be taken, and which additional capabilities are needed.

4. Leverage public-private partnerships and multi-stakeholder efforts to incentivize the adoption and deployment of secure IoT devices

Private-public partnerships are an important mechanism to incentivize the adoption and deployment of secure IoT devices. Public-private partnerships combine government, academic and private sector resources to facilitate research, leadership, and governance to help advance IoT. Industry, together with government and academia, has been tremendously active in developing IoT security best practices. NIST’s IoT device security capability core baseline, NISTIR 8259A, is a key example of such an effort. The C2 Consensus maps nicely to the NIST work; C2 is a “multi-sector core baseline” that extends the NIST “core baseline”. Similarly, industry successfully collaborated with the Department of Commerce on efforts to create its 2018 Botnet Report and subsequent update.¹⁴ The IT Sector Coordinating Council (IT-SCC) is tracking the Botnet Road Map with activities that implement the recommendations. Policymakers should further consider supporting multi-stakeholder efforts as well as studying and addressing potential barriers to international standards development in these domains. Successful public-private sector collaboration should provide ample time for consultation and seek to avoid duplicative or counterproductive and conflicting regulatory approaches.

By way of example, NIST has further developed contributions to the international standard on IoT device baseline security requirements (ISO/IEC 27402, in development), based on NISTIR 8259A, to support the development of harmonized approaches.¹⁵

5. The heterogeneity and complexity of the IoT merits a thoughtful and holistic approach to device security

The diverse and complex nature of the IoT landscape merits a thoughtful and holistic approach to policymaking. Connected devices and technical supply chains are intertwined. Policies to regulate the IoT must therefore comport with policy and security principles underpinning domains that closely interact with this ecosystem, such as cloud security, consumer products, 5G, and telecom security. Such policies must also consider existing and evolving risk-frameworks and trustworthy supply chain policies. Policymakers should consider security practices that may extend beyond the observable device characteristics, such as risk assessment and secure development. Notably, consensus-driven reports and international standards can be leveraged in these domains as well (see, e.g., ISA/IEC 62443, and ISO/IEC 27000 series).


6. Consider existing Self Attestation and Conformity Assessments by Suppliers/Vendors as alternative for Certification

Policymakers have proposed a variety of IoT security regulations and policies, ranging from self-attestation to 3rd-party certification and labeling schemes. Industry and expert groups have developed principles that apply more broadly that can be considered in this regard, yet go beyond the scope of this document. The below is a non-exhaustive list of resources that highlight the potential complexity associated with proposed regulatory approaches to certification and labeling, including from a consumer usability perspective:

- ▶ CTA Smart Policy to Secure Our Smart Future: How to Promote a Secure Internet of Things for Consumers, <https://www.cta.tech/Resources/Newsroom/Media-Releases/2021/March/IOT-Device-Security-White-Paper-Release>
- ▶ U.S. Chamber of Commerce Principles for IoT Security, <https://www.uschamber.com/IoT-security>
- ▶ ITI Policy Principles for Cybersecurity Certification, https://www.itic.org/policy/ITI_PolicyPrinciplesforCybersecurityCertification_Final.pdf
- ▶ ITI IoT Security Policy Principles, <https://www.itic.org/dotAsset/d9c7be68-d2d4-42de-aaea-e91fc526b717.pdf>
- ▶ BSA Policy Principles for Building a Secure and Trustworthy Internet of Things, https://www.bsa.org/files/policy-filings/07022002iotsecpolicyprinciples_0.pdf

The proliferation of mandatory certification or labeling is said to be a necessary step towards ensuring device security in light of the rapidly growing and diverse IoT landscape. To the contrary, security is enhanced by policies that preserve flexibility and allow for alternative approaches to demonstrating compliance, such as flexible adoption of standards. This ability to leverage multiple alternatives is instrumental since many valid approaches are used by vendors globally to address security risks. These mechanisms are recognized and accepted by the marketplace, and industry has the requisite experience. These approaches also respond to the need for solutions that are globally harmonized, agile, mutually recognized, and are consistent with risk-based approaches for security.

One-size-fits-all approaches such as mandatory labeling or 3rd party certification requirements could lead to slowdowns in product development, ultimately harming companies seeking to deploy products and security solutions in a global marketplace. Eschewing a one-size-fits-all approach in favor of a more flexible model will



limit the costs that must be borne by vendors and are ultimately passed along to consumers and will avoid delays or constraints in the deployment of IoT solutions due to duplicative and fragmented requirements. More, as discussed above, overly prescriptive rules can hinder device interoperability, scalability, and innovation. Given the dynamic and complex nature of the IoT, it is unlikely that static labeling or certification approaches would be effective to address security rapidly evolving security threats. Utilizing industry's experience in varied approaches increases the security delivered to the marketplace as a whole.

A non-exhaustive list of proposed/enacted regulations includes:

- ▶ The IoT Cybersecurity Improvement Act (passed) and implementing guidelines in development (e.g. NISTIR 8259 Federal profile set of documents including NISTIR 8259D (in draft))
- ▶ U.S. Cyberspace Solarium Commission proposed U.S. Federal Legislation
- ▶ State Legislation in U.S. on Connected Devices (CA, OR, proposed in other states)
- ▶ Amendments to the RED Directive (EMEA) (proposed, evolving)
- ▶ ENISA proposed certification schemes for ICT products, services, and processes, to include the IoT landscape and proposed “horizontal” policy effort for connected products contemplated
- ▶ Proposals for regulating consumer smart product cyber security (United Kingdom: The Department for Digital, Culture, Media and Sport) and related ETSI EN 303-645 standard development activities
- ▶ Proposed regulations in Brazil (ANATEL) (Terminal Equipment)
- ▶ Proposed Certification requirements for Security of Terminal Equipment in India
- ▶ The Ministry of Economy, Trade and Industry (METI) Cyber/Physical Security Framework pertaining to the security of IoT and other connected systems and technical standards for IoT Security (Japan Ministry of Internal Affairs and Communications)
- ▶ Guidelines for Standard Certification of Terminal Equipment based on Telecommunications Business Act (April 22, 2019)
- ▶ Proposed regulation in Malaysia
- ▶ Singapore: The Infocomm Media Development Authority is developing an IoT Cyber Security Guide
- ▶ Specific guidelines issues for telecom equipment in Germany
- ▶ Australia, the Department of Home Affairs, Draft Code of Practice: Securing the Internet of Things for Consumers and more

Endnotes

1 C2 brought together trade associations, standards development organizations, industry alliances and coalitions to develop the C2 Consensus Baseline published in September 2019 and expanded in the CSDE's 2020 International Botnet and IoT Security Guide. Each group represents anywhere from dozens to thousands of companies. A number of the groups are international in scope. The technical expertise in the Consensus is informed, therefore, by a global legion of industry security professionals. The Consensus cannot capture the perspectives and capabilities of all parts of the IoT ecosystem, but it recognizes a few key baselines that can be commonly pursued and flexibly implemented by manufacturers and others that are looking for guidance. The Consensus articulates the accepted commonalities in IoT device security and identifies the areas where consensus has not yet developed.

2 NISTIR 8259A IoT Device Cybersecurity Capability Core Baseline (2020), available at <https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8259A.pdf>.

3 ISO/IEC JTC 1/SC 27 27402 (“Cybersecurity — IoT security and privacy — Device baseline requirements”) in Working Draft (CD stage) (2020), more information on the status of the standard is available at <https://www.iso.org/committee/45306.html>

4 CTA-2088 Baseline Cybersecurity Standard for Devices and Device Systems (2020), available at <https://shop.cta.tech/collections/standards/products/baseline-cybersecurity-standard-for-devices-and-device-systems-cta-2088>.

5 See the non-exhaustive list of proposed/enacted regulations on page 5.

6 These incentivization mechanisms can include procurement processes that prioritize interoperable and scalable IoT security features, on voluntary basis, which adopt industry-led, consensus-driven, international standards.

7 A Supplement to the C2 Consensus that reaffirms the 2019 document and updates mappings will be available in late 2020 at <https://CSDE.tech>.

8 This definition includes defined terms such as transducer (sensor or actuator) and network interface. See NISTIR 8259, at 1.

9 Compare to the recently passed IoT Cybersecurity Improvement Act, in the United States: “[C]onsistent with the second draft National Institute for Standards and Technology Interagency or Internal Report 8259 titled “Recommendations

for IoT Device Manufacturers: Foundational Activities and Core Device Cybersecurity Capability Baseline”, published in January 2020, Internet of Things devices are devices that (A) have at least one transducer (sensor or actuator) for interacting directly with the physical world, have at least one network interface, and are not conventional Information Technology devices, such as smartphones and laptops, for which the identification and implementation of cybersecurity features is already well understood; and (B) can function on their own and are not only able to function when acting as a component of another device, such as a processor”. See also ETSI EN 303-645 (consumer IoT) defining “device manufacturer” as the entity that creates an assembled final consumer IoT product, which is likely to contain the products and components of many other suppliers”.

10 See, e.g., CTIA's IoT Cybersecurity Certification program, <https://api.ctia.org/wp-content/uploads/2019/03/CTIA-Certification-FAQ-Ver-1.0-28-March-2019.pdf>; GSMA IoT Security Assessment, <https://www.gsma.com/iot/iot-security-assessment>.

11 *The C2 Consensus on IoT Device Security Baseline Capabilities*, at 8.

12 See NISTIR 8259 (Draft 2nd) at 7: “Manufacturers cannot completely understand all of their customers’ risk because every customer faces unique risks based on many factors”.

13 Examples of standards and reports emerging for risk profiling (the process of creating a risk profile for a certain vertical) include: IEC 31010:2019; Risk management — Risk assessment techniques, ISA/IEC 62443, NISTIR 8259C (draft). See also ISO/IEC 27001.

14 Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats, <https://www.ntia.doc.gov/press-release/2018/us-departments-commerce-homeland-security-release-report-president-promoting>; Botnet Roadmap Status Update, https://www.ntia.gov/files/ntia/blogimages/botnet_road_map_status_update.pdf.

15 NIST, “More than just a milestone in the Botnet Roadmap towards more securable IoT devices”: “What’s Next for the Core Baseline?... We plan to continue to participate in the International Organization for Standardization (ISO)/IEC project to develop an international standard for an IoT device baseline of security requirements.”), <https://www.nist.gov/blogs/cybersecurity-insights/more-just-milestone-botnet-roadmap-towards-more-securable-iot-devices>.



Council to Secure the
Digital Economy

securingdigitaleconomy.org