Before the
National Institute of Standards & Technology
Washington, DC

In the Matter of	)	
	)	
Foundational Cybersecurity Activities	)	NIST IR 8259 Rev. 1
for IoT Product Manufacturers	)	
	)	

COMMENTS OF USTELECOM – THE BROADBAND ASSOCIATION

USTelecom – The Broadband Association ("USTelecom")[1] respectfully submits these comments in response to the National Institute of Standards and Technology ("NIST") public draft of NIST IR Rev. 1, *Foundational Cybersecurity Activities for IoT Product Manufacturers*.[2] USTelecom is encouraged by NIST's continuous commitment to securing the Internet of Things ("IoT"), and we appreciate NIST's partnership toward this shared goal for nearly a decade.

This publication represents another important milestone in advancing IoT security. As NIST finalizes this revision, we respectfully offer two overarching considerations. First, focusing on "IoT products" rather than individual devices introduces implementation challenges that could inadvertently delay or hinder adoption of the guidance. Second, we recommend maintaining a clear distinction between cybersecurity and privacy guidelines. Blurring these domains may limit the practical application of the guidance, as organizations with varying privacy policies might find it difficult to align with requirements that conflate the two.

[1] USTelecom is the nation's leading trade association representing service providers and suppliers for the telecom industry. USTelecom members provide a full array of services, including broadband, voice, data, and video over wireline and wireless networks. Its diverse member base ranges from large international publicly traded communications corporations to local and regional companies and cooperatives, serving consumers and businesses in every corner of the country and world.

[2] NIST IR 8259 Rev. 1 (Initial Public Draft), *Foundational Cybersecurity Activities for IoT Product Manufacturers*, https://nvlpubs.nist.gov/nistpubs/ir/2025/NIST.IR.8259r1.ipd.pdf.

Focusing on "IoT Products" Creates Implementation Challenges. A focus on IoT *products*—as opposed to discrete *devices*—risks undermining security by misaligning control with responsibility. In a typical IoT deployment, the "product" often encompasses multiple components: a physical device, firmware, connectivity modules, mobile applications, and cloud-based services. These components are frequently developed and maintained by different entities across a fragmented supply chain.

Crucially, device manufacturers often lack visibility into, or control over, other elements of the product ecosystem, such as backend infrastructure or third-party mobile apps. For instance, a hardware vendor may implement secure boot, memory protection, and cryptographic operations on the device itself—but has no authority to enforce identity management practices or logging policies in a companion cloud service operated by a different organization. If security guidance is framed around the *entire product*, then the manufacturer may be deemed non-compliant despite having implemented all applicable controls within their scope.

This misalignment creates two technical problems:

1. **Diffusion of responsibility**: No single actor can guarantee that the entire "product" conforms to NIST's recommendations. This creates gaps in implementation coverage, especially where contractual or organizational boundaries prevent coordinated security practices across components.
2. **Implementation bottlenecks**: Organizations may delay or avoid adopting security practices altogether if they believe full conformance depends on integrating with external parties or systems they don't control. This can hinder incremental security improvements that could otherwise be made at the device level.

In contrast, a device-centric approach allows each actor in the supply chain to apply specific, technically enforceable controls within their domain without being held accountable for adjacent systems beyond their reach. Security outcomes improve when each stakeholder can independently implement and verify controls aligned with their technical authority.

Keeping Cybersecurity and Privacy Guidance Distinct Encourages Broader Adoption. While cybersecurity and privacy are interrelated, conflating them as "foundational cybersecurity activities" can create confusion—and more importantly obstacles—to adoption. Cybersecurity guidance should focus on technical and organizational safeguards to protect the integrity, availability, and confidentiality of systems. Privacy practices, on the other hand, often depend on legal, cultural, or sector-specific requirements that vary significantly between jurisdictions and organizations.

Embedding privacy-specific expectations into foundational cybersecurity guidance risks limiting the audience able or willing to implement the recommendations, particularly in global or multi-jurisdictional markets. We recommend that privacy be acknowledged as an important, complementary concern—but addressed through distinct, parallel frameworks where organizations can align security controls with their respective privacy obligations without creating compliance conflicts.

By maintaining clear boundaries between cybersecurity and privacy domains, NIST can better ensure that its guidance remains widely usable, technically actionable, and aligned with the core objective of promoting secure-by-design IoT practices.

We thank NIST for the opportunity to weigh in regarding these matters and look forward to continued partnership.

Respectfully submitted,

/s/ Paul Eisler

Paul Eisler
Vice President, Cybersecurity

USTelecom – The Broadband Association
601 New Jersey Avenue, NW
Suite 600
Washington, DC 20001
(202) 326-7300

July 14, 2025