

Security in the Billions

Securing Consumer IoT Products

Presentation by Justin Sherman and Patrick Mitchell

NIST IoT Advisory Board

January 19, 2023

Report by Patrick Mitchell, Liv Rowley, and Justin Sherman
with Nima Agah, Gabrielle Young, and Tianjiu Zuo for the Atlantic Council

Data Driven - Comprehensive IoT Survey

International Focus – Four Countries

- United States, United Kingdom, Australia, Singapore

Private Sector Security Efforts

Industry Organization Security Efforts

Risks and Activities Across Three Verticals

- Smart homes
- Networking gear
- Consumer health

Current Methods

Government procurement

Voluntary Code of Practice

Mandatory minimum standards

Industry guidance

Country-wide labeling

Current Hurdles



Challenges for State

Fragmented approach across jurisdictions

Fragmented approach *within* jurisdictions



Challenges for Private Sector

Ambiguous requirements and policy goals

Diverging process and regulatory requirements

Duplicative certification schemes

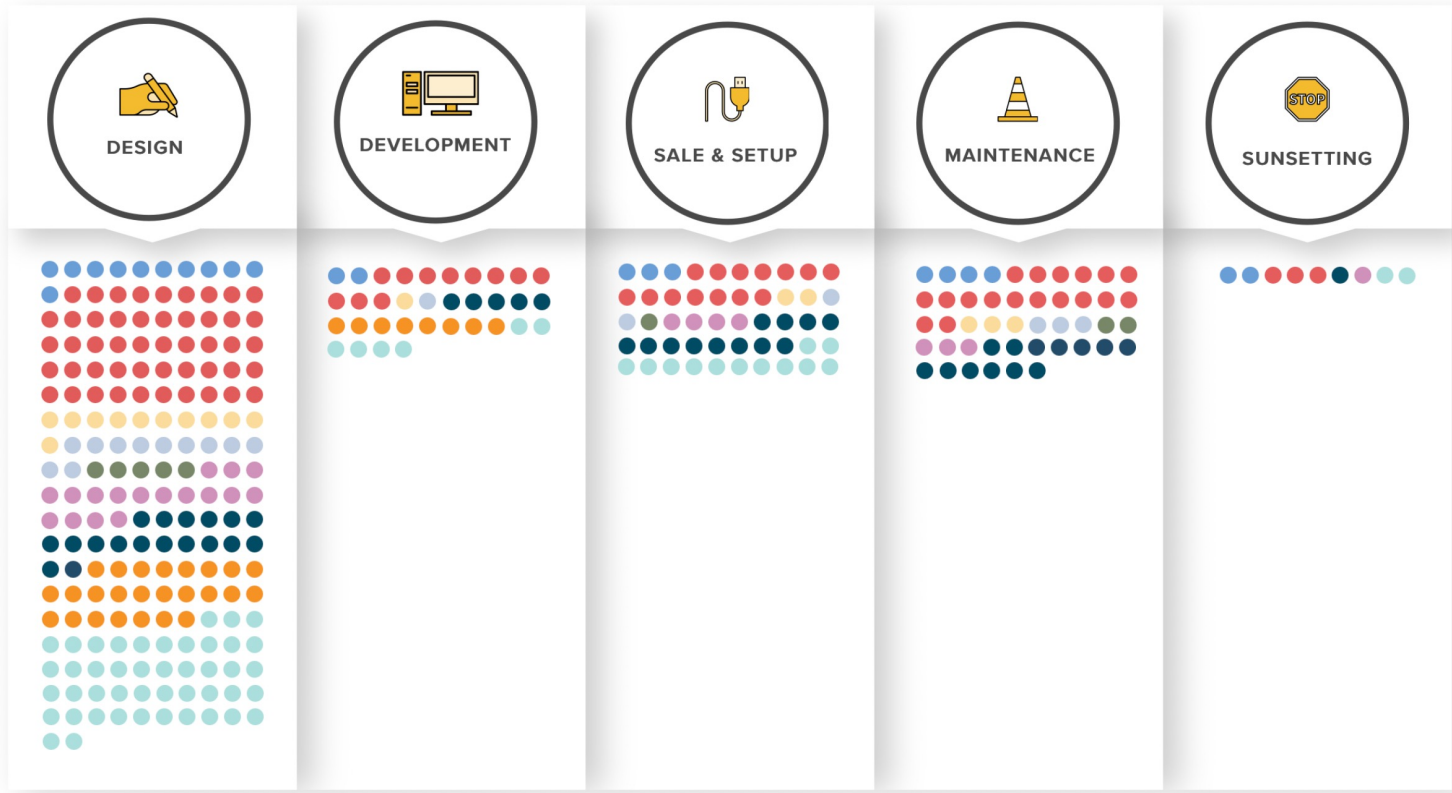
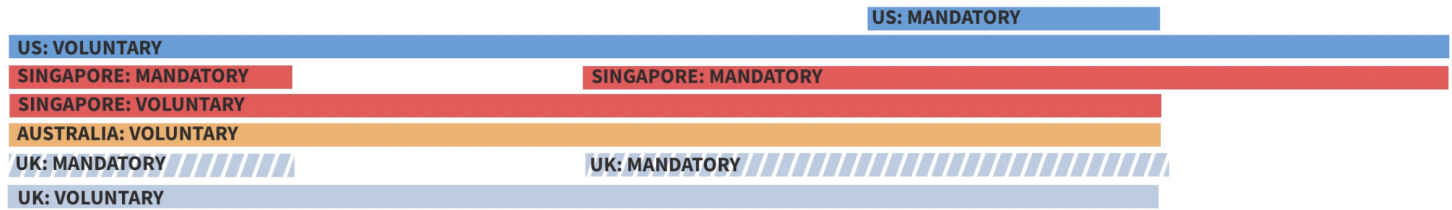


Challenges for Users

Little to no information to make good buy-side choices

Bad security outcomes/insecurity

Harmful knock-on effects



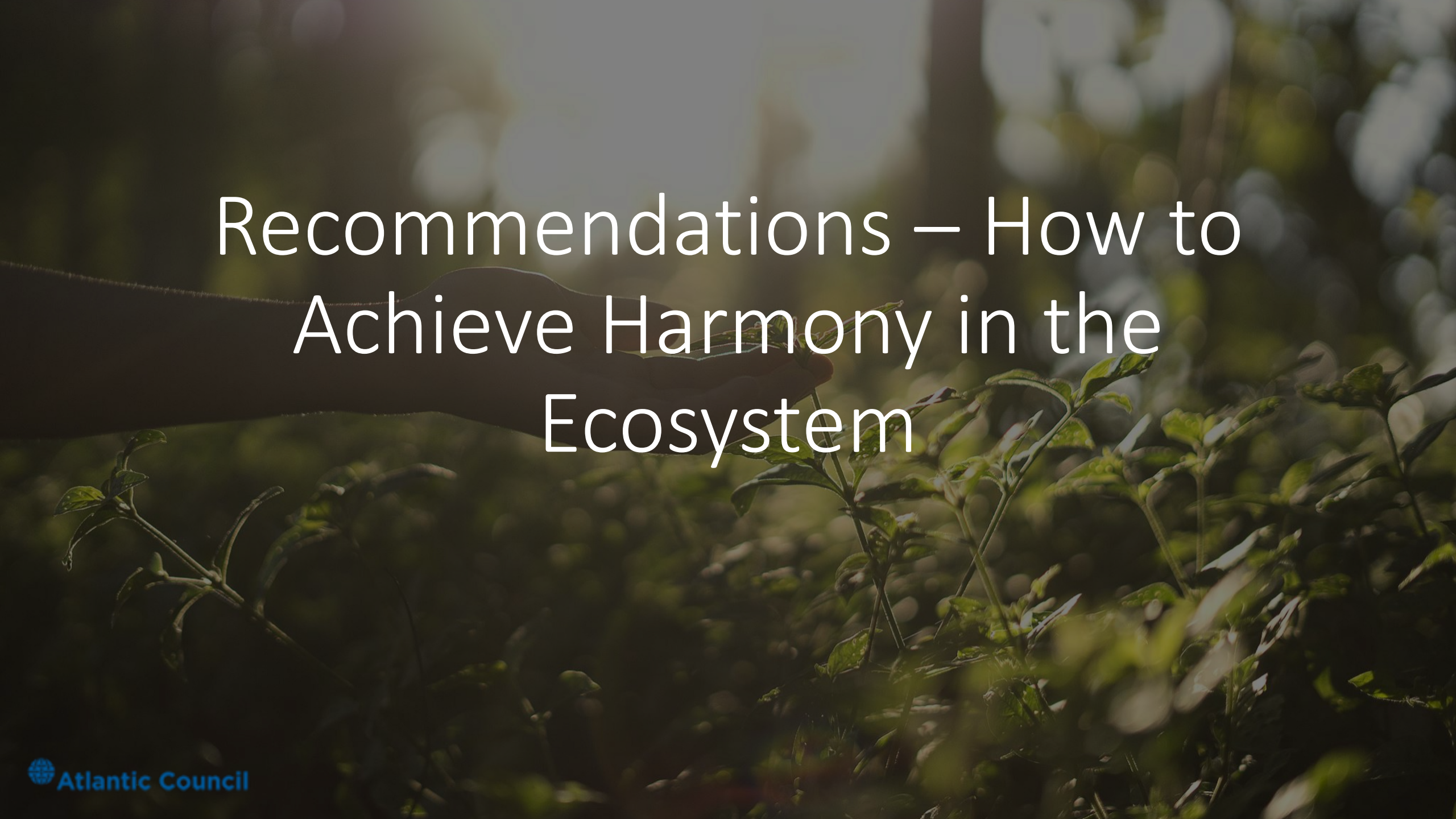
Governments have various tools in their toolbox to promote consumer IoT product security.

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

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

- Government:**
- United States
 - Singapore
 - Australia
 - United Kingdom

- Industry Frameworks:**
- ioXt
 - CSDE
 - AGELIGHT
 - App Defense Alliance
 - ETSI EN 303 645

A hand holding a small plant against a background of a forest with sunlight filtering through the trees.

Recommendations – How to Achieve Harmony in the Ecosystem

Our Approach



Tiers (of security measures)



Recommendations (country-agnostic implementation)



US guidance (specific implementation)

Tier 1 – Minimum Baseline Features

Mandatory baseline to ensure IoT products have most basic and critical security measures in place

Set by government agency responsible for cybersecurity standards

Should be rooted in widely agreed upon standards, such as ETSI EN 303 645

Manufacturers self-attest to meeting standards

Receipt of label for compliant device

Random government audits to ensure compliance

Tier 2 – Enhanced Security Features

Standards above baseline

Result of government consultation with industry

Draw inspiration from international standards such as ETSI EN 303 645

Labels are independently verified through a quick and cheap process

Receipt of label for compliant device

Special Standards for Safety Critical Products

Set by industry-specific regulators

Highest bar of security standards
for products that could impact
human life

No accompanying label

Labels



Physical & digital



Consider cooperating with industry, academic, civil society on design



Aimed at individuals and enterprise



Clearly articulate information



Mutually recognized across jurisdictions

Recommendation Sets

- **Set the Baseline of Minimally Acceptable Security (Tier 1)**
 - Recommendation 1: Governments should implement regulatory measures to enforce a mandatory baseline on manufacturers selling in their markets.
 - Recommendation 2: Governments should follow the “reversing the cascade” philosophy, where instead of trying to influence manufacturers based abroad, governments put pressure on domestic suppliers and retailers—who may, in turn, put their own pressure on manufacturers to improve security.
- **Incentivize Above the Baseline (Tier 2)**
 - Recommendation 3: Governments should support the creation of a voluntary, higher tier of security requirements, indicated via labeling programs in their markets.
 - Recommendation 5: In the short term, governments should reach agreements to mutually recognize each other’s labels.
- **Pursue international alignment on standards and implementation that cover entire lifecycle**
 - Recommendation 7: Governments should pursue outcomes-based approaches to consumer IoT security rooted in agreed-upon basic security principles and maintain similar definitions for products considered “in-scope.”

US Specific Guidance

Set the Baseline of Minimally Acceptable Security

- States should pass and enforce their own IoT security laws.
- The federal government should adopt the binary labeling approach proposed by NIST.

Incentivize Above the Baseline

- Provide incentives for industry to obtain labels.
- Provide liability protection for firms that pursue the higher, tier 2 security standards.

“That’s all Folks!”



For more information, reach out to us at therr@atlanticcouncil.org!